UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de riesgos y seguridad de la información del Programa Fortalece Perú del MTPE, 2019

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Ingeniería de Sistemas con mención en Tecnologías de la Información

AUTORA:

Br. Lourdes Harumi Calderon Taboada (ORCID: 0000-0003-1074-046X)

ASESOR:

Mg. Luis Alberto Torres Cabanillas (ORCID: 0000-0003-2808-7753)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

Lima – Perú

2019

Dedicatoria

A Dios por haberme permitido llegar hasta acá bendiciéndome con salud y sabiduría.

A mi querida madre por siempre brindarme todo su amor, ánimos y apoyo incondicional.

Agradecimiento

A todos los docentes de la Escuela de Posgrado de la Universidad César Vallejo, quienes fueron parte de mi formación profesional.

A mi asesor de tesis, por su esfuerzo y dedicación contribuyeron en la elaboración de mi tesis.

Página del Jurado

Declaratoria de autenticidad

Yo, **Lourdes Harumi Calderon Taboada**, estudiante de la Escuela de Posgrado, Maestría en Ingeniería de Sistemas con mención en Tecnologías de la Información, de la Universidad César Vallejo, Sede Lima Norte; declaro el trabajo académico titulado "**Gestión de Riesgos y Seguridad de la Información del Programa Fortalece Perú del MTPE, 2019**" presentada, en 99 folios para la obtención del grado académico de Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información, es de mi autoría.

Por tanto, declaro lo siguiente:

He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.
No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinen el procedimiento disciplinario.

Lima, 10 de agosto del 2019

Lourdes Harumi Calderon Taboada

DNI: 47650978

Índice

Índice de Tablas

Pág.

Índice de Figuras

Pág.

Resumen

El siguiente trabajo de investigación, tiene como objetivo principal determinar la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019. Donde el estudio fue de tipo básico nivel descriptivo correlacional, no experimenta de corte transversal, con una población y muestra de 25 consultores del Programa Fortalece Perú. Se aplicó el método hipotético deductivo bajo el enfoque cuantitativo y se realizó el procesamiento de datos con el software estadístico SPSS, donde el valor del coeficiente Alfa de Cronbach es 0.753 o 75.3% obtenido de 22 ítems de la variable Gestión de Riesgos, y 0.753 o 75.3% resultante de 14 ítems de la variable de Seguridad de Información. Los valores obtenidos nos indicaron que la confiabilidad fue fuerte para las variables, asimismo, del juicio de expertos se es afirmativa en la validación por los tres expertos, entendiéndose que el instrumento (cuestionario) fue confiable y aplicable a la población de estudio.

Se determinó que existe una relación directa y significativa de nivel medio entre la gestión de riesgos y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.661. Por ello, se propuso el uso de las metodologías de ambas variables para que asegure la continuidad del negocio.

Palabras clave: Gestión de riesgos, seguridad de la información, continuidad del negocio.

Abstract

The main objective of the following research work is the relationship between Risk Management and information security of the Fortalece Perú Program of the MTPE, 2019. Where the study was a basic descriptive-level correlational level, it does not experience a cross-section, with a population and sample of 25 consultants of the Strengthens Peru Program. The hypothetical deductive method was applied under the quantitative approach and the data processing was carried out with the statistical software SPSS, where the value of the Cronbach's Alpha coefficient is 0.753 or 75.3% of 22 items of the variable Risk Management, and 0.753 or 75.3% resulting from 14 items of the Information Security variable. The values included in the validation of the three experts, as well as the instrument (questionnaire), are reliable and applicable to the study population.

It was determined that there is a direct and significant mid-level relationship between risk management and information security of the Strengthening Peru 2019 Program, resulting in Spearman's Rho = 0.661. Therefore, the use of the methodologies of both variables was proposed to ensure business continuity.

Keywords: Risk management, information security, business continuity.

I. Introducción

En las organizaciones, el factor tecnológico es un valor importante que puede influir en su crecimiento organizacional y económico. En los últimos años, se ha podido notar un creciente avance tecnológico, encontrándonos cada día con nuevas herramientas sofisticadas y con más funcionalidades, así como también, herramientas para influir maliciosamente en la seguridad de la información, el riesgo tecnológico siempre estará presente. Y por lo general, las víctimas se enteran que han sido afectadas después de mucho tiempo y en algunos casos cuando ya es demasiado tarde. Por ello, es importante reconocer los tipos de riesgos y afrontarlos de la mejor manera posible con el apoyo de metodologías y herramientas que ayuden a su fin. Anderson, Baskerville y Kaul (2017) comentan "Dos fenómenos opuestos crean una tensión esencial en los sistemas de información: la necesidad de compartir información y proteger la información. Los avances tecnológicos han mejorado la capacidad de compartir e intercambiar información de manera más eficiente, pero que también aumenta la carga de asegurar esta información" (p. 2). Según Mäntykangas (2018) "existe una relación entre el usuario de la información y los sistemas de información. Esta relación puede ser vulnerable a los riesgos inherentes a ella" (p. 1). Hu, West y Smarandescu (2015) "Definimos la violación de la política de seguridad como cualquier acto donde un empleado que usa computadoras y que están en contra de las reglas y políticas, como por ejemplo: acceso no autorizado a datos y sistemas, copia no autorizada o transferencia de datos confidenciales o la venta de datos para obtener ganancias personales" (p. 3). Chatterjee, Sarker y Valacich (2015) "el mal uso de los sistemas informáticos tiene el mayor potencial de pérdida y daño a el empleador" (p. 3).

Martelo, Madera y Betín (2015) "la información de una organización cuando está completa, precisa y actualizada es fundamental en la toma de decisiones de las mismas" (p. 2). Molina comenta "Los riesgos están presentes en todo ámbito laboral y pueden provocar muchas pérdidas en el negocio si no son controladas a tiempo y de forma adecuada" (p. 1). Martínez, Martínez, Mud, Mud, Moreno, Martínez (2015) Sugieren que "aquellas aplicaciones desarrolladas por equipos multidisciplinares son las que deben contener mayor calidad y seguridad de la información" (p. 3). Zhang y Yang (2018) "El factor humano es una importante dimensión en todos los problemas relacionados con la seguridad" (p. 1). Wang, Shan, Manish y Raghav (2019) mencionan "Las amenazas internas representan un riesgo significativo para una organización. Según el informe de amenazas internas el 89% de las organizaciones encuestadas cree están en riesgo de ataques

internos" (p. 2). También, Barlow, Warkentin, Ormond y Dennis (2018) comentan "las organizaciones deben protegerse contra vulnerabilidades de ataques externos y cumplir con la seguridad externa y reglas de privacidad, aunque muchas de las vulnerabilidades de seguridad surgen de las acciones de empleados" (p. 1). Hadlington y Parsons (2017) "el elemento más débil en la cadena de ciberseguridad es el usuario final humano. Alineado con esto hay investigaciones previas que indican que mejorar la conciencia de seguridad de la información de los empleados es clave para proteger a las organizaciones" (p. 1). Kobek y Caldera "la privacidad es un concepto dinámico que se puede adaptar a la necesidades y valores de los individuos" (p.3). Carol, Jae Nam y Straub (2012) "La privacidad debe tener la máxima importancia porque está en transición analógico a digital, incluso cuando la información está fácilmente disponible y fácilmente accesible" (p. 1).

En Madrid, Romeral y Torres (2008) afirmaron que, "Un punto importante es la gestión de riesgos tecnológicos. Permiten a la organización tener una visión detallada y exacta de los riesgos, y constituyen una buena herramienta de decisión acerca de qué riesgos pueden ser gestionados en un entorno de recursos limitados." (p. 14). Arévalo, Bayona y Rico (2015) comentan "Las organizaciones deben generar un plan de acción frente a las amenazas. Este plan es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación. Se hace de manera formal en la norma ISO 27001, donde se recogen los estándares y mejores prácticas de seguridad de la información" (p. 2). Para Cram, D'Arcy y Proudfoot (2019) "una táctica que las empresas usan para proteger sus sistemas y datos es la creación, implementación y aplicación de políticas de seguridad de la información" (p. 1). Georg (2017) "Una razón para enfocarse en la seguridad de la información es que se trata particularmente asuntos legales delicados que podrían presentar riesgos significativos por falta de legalidad" (p. 3). Para Li y Wang (2019) "La tecnología de seguridad de la información puede garantizar efectivamente el almacenamiento de seguridad de la información del centro de datos informáticos" (p. 2). Singh y Margam (2018) comentan "implementar seguridad de la información para proteger sus activos de todas amenazas potenciales para garantizar la confidencialidad, integridad y disponibilidad de sus recursos de información" (p. 1). Los estándares de seguridad de la información basados en el cumplimiento de controles, se focalizan en disminuir las vulnerabilidades y los riesgos, internos y externos, que afectan los activos de información. Aguilera, Pérez y

Rivero (2017) afirmaron que, “La seguridad de la información es un proceso continuo que debe ser controlado, gestionado y monitorizado en el que la caracterización de las TI juega un importante papel dentro de la gestión global de la seguridad de la información” (p. 46). Miloslavskaya, Lima y Rocha (2018) comentan “Un nivel suficiente de Seguridad de la Información (SI) de una organización se debería mantener durante mucho tiempo para contrarrestar amenazas, reducir los riesgos y procesar eficientemente eventos e incidentes” (p. 2). Boateng, Coffie y Hayford (2018) “La confianza ha sido un aspecto clave en las organizaciones. Sin embargo, dentro del sector público como un medio de crear conciencia de seguridad sufre un tratamiento riguroso y sistemático” (p. 1).

En el Programa “Fortalece Perú” del Ministerio de Trabajo y Promoción del Empleo, tiene como objetivo el mejoramiento y ampliación de los servicios del Centro de Empleo (CE) para la inserción laboral formal de la población juvenil económicamente activa en 7 regiones del Perú; esperando mejorar la efectividad, eficiencia y pertinencia de los servicios que ofrecen los CE para fortalecer la articulación de los jóvenes urbanos con las empresas privadas buscadoras de trabajadores. Un especialista en TI puede percibir claramente lo vulnerable y expuesta que se encuentra la información física y virtual y los posibles riesgos que pueden intervenir en el cumplimiento de los objetivos del Programa si no se toman las medidas de seguridad que corresponden. En primera instancia, no existe el análisis de los procesos tecnológicos que muestre los niveles riesgos identificados, evaluados, monitoreados y controlados. Carece de metodologías de gestión de riesgos que garantice la continuidad operativa ante amenazas de la seguridad de la información, no existen políticas de restricciones de accesos a la información, no se cuenta con un encargado que administre y vele por la información del Programa.

Crespo, Carvajal, Astudilo, Orellana, Vintimilla y Carvallo “La seguridad de la información es una preocupación creciente en empresas y organizaciones, siendo más alta aun cuando se vincula a plataformas financieras donde existe información sensible” (p. 1). Para Mitkovskiy, Ponomarev y Proletarskiy (2019) “el oficial de seguridad de la información crea reglas de correlación y normalización para el tráfico de red, investigue incidentes, clasifique amenazas y priorizarlos, configurar filtros” (p. 51).

El propósito del trabajo de investigación es determinar la relación entre las variables gestión de riesgos y la seguridad de la información, para ello se utilizará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) para el diagnóstico de la primera variable, y la metodología de seguridad de la información ISO

27001 para la segunda variable. Con la finalidad de conocer detalladamente y tener el mapeo de los niveles de riesgos y amenazas a las que se encuentra expuesta los activos de la información y conocer el impacto que podría causar. Siendo necesario identificar y analizar los riesgos tecnológicos para que aseguren la seguridad de la información y la continuidad operativa. Para ello, se recogerá información de diversas fuentes (personas, presupuesto, requisitos, necesidades, etc.)

Molina (2015) en su investigación titulada Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral. El objetivo fue aminorar las fallas y amenazas que irrumpe la seguridad de los equipos de cómputo, servidores y de la información, se basaron en la metodología MAGERIT para conocer y mapear las amenazas a los cuales se encontraban expuestos los activos de la información. El tipo de estudio aplicada, bajo un enfoque cualitativo. El instrumento usado fue encuestas al personal. La investigación dio como resultado que las propuestas de las medidas de seguridad ayudaron a minimizar los riesgos de las amenazas físicas de manera correcta y oportuna.

Mina (2015) en su investigación titulada Auditoria de seguridad de la información e infraestructura de TI, al área de TI de la empresa de energía de ARAUCA ENELAR E.S.P. del departamento de Arauca. La problemática fue la falta de auditorías en TI que le permita identificar los distintos riesgos a los que estaban expuestos sus activos. El objetivo fue realizar una auditoria TI que permita identificar los activos con que cuenta la entidad, las amenazas a que están expuestos y posteriormente, se dar las recomendaciones pertinentes que permitan salvaguardar la información y la infraestructura de TI de la organización. La metodología que se usó son las dos primeras fases del ciclo PDCA (Plan-Do-Check-Art) para el cumplimiento de Seguridad de la Información, la metodología MAGERIT para el cumplimiento de la gestión de riesgos. El Tipo de estudio aplicada, bajo el enfoque cuantitativo y cualitativo. La población lo conformó 9 personas, mientras que la muestra de seleccionada es Subdirector de sistemas, informática y telecomunicaciones, Coordinador de sistemas, informática y telecomunicaciones y Contratista de apoyo desarrollo de software. Los instrumentos para recopilar información fue el checklist y el cuestionario. Como conclusiones, luego de realizada la auditoria se evidenciaron una serie de factores que ponen en riesgo los activos de información de la empresa, entre ellos se encuentran los bajos controles de acceso físico desplegados para evitar el acceso de

personas no autorizadas a las áreas de procesamiento de información, ésta incidencia aumenta la probabilidad de perdida, deterioro e indisponibilidad de la información y los equipos de cómputo. Así mismo, la inadecuada gestión de los activos de información debida a la falta de prácticas para su uso adecuado, no tener definidas las responsabilidades del personal sobre ellos, ni tener establecidos controles que garanticen su devolución al finalizar el contrato laboral de los empleados.

Tola (2015) en su investigación titulada Implementación de un sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría, aplicando la norma ISO/IEC 27001. El proyecto reunió la información necesaria para la implementación de un Sistema de Gestión de la Seguridad de la Información, basado en la norma ISO 27001:2005, para garantizar la protección de los activos de información y otorgar confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La correcta implementación de un SGSI dentro de las empresas, ayudó a prevenir incidentes de seguridad, que generan pérdidas económicas e interrupciones en la continuidad de negocio, mediante la reducción de las probabilidades o impactos que los riesgos identificados pudieran ocasionar a su información. Investigación Aplicada, bajo el enfoque cuantitativo.

Fernández y Monteros (2014) Propuesta metodológica para la gestión de riesgos tecnológicos en empresas proveedoras de servicios de telecomunicaciones. Su objetivo fue establecer una propuesta metodológica para gestionar los riesgos tecnológicos en empresas Proveedoras del Servicio de Internet (ISP). Ésta nace de una investigación previa realizada al sector, en empresas autorizadas a operar y brindar el servicio en la ciudad de Quito, para lo cual, se tomó como referencia el estándar internacional de control: COBIT 4.1. como resultado se determinó un nivel relativamente bajo de madurez con el que dichas empresas gestionan los riesgos de Tecnologías de la Información. Adicionalmente, los análisis de otros marcos de referencia como: MARGERIT v3, ISO/IEC 27005: 2012 y las Guías de Auditoría de Tecnología Global GTAG. El tipo de estudio aplicada. En cuanto a la población encuestada, se debe indicar que conociendo todas las empresas ISP autorizadas para proveer servicios en la ciudad de Quito (datos SUPERTEL), se procedió a contactar al personal técnico de cada una con la encuesta en mención. Es decir, se contactaron a las 57 empresas ISP de Quito, recibiendo la respuesta de 13. Su instrumento fue la encuesta.

Otoya (2018) Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017. Agrorural vela por la correcta atención de servicios públicos agrarios, en este contexto es de vital importancia el manejo de la

información de manera correcta y oportuna para las mejores decisiones, por lo que fue necesario identificar, analizar y tratar los riesgos tecnológicos que permitan un adecuado sistema de seguridad de la información que asegure la continuidad operativa y poder contar con la disponibilidad de la información de manera confidencial e integra. Existe la disponibilidad y obligatoriedad de establecer el SGSI (sistema de gestión de seguridad de la información) según la (ONGEI, 2009) pero hay poca importancia de desarrollar planes de actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo en las diferentes Instituciones Nacionales de la cual no es ajena Agrorural, por lo que la seguridad de la información necesitaba de un proceso de gestión del riesgo es decir, una aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo. Se realizó una investigación básica nivel descriptivo con un diseño no experimental corte transversal, bajo el enfoque cuantitativo. La población estuvo conformada por 174 colaboradores y la muestra de 120 individuos. El instrumento que el autor utilizó para la recaudación de información fue el cuestionario. Una de sus conclusiones fue que existe una influencia significativa de la gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017 de un nivel alto teniendo este un valor de significancia de 0.035 y una dependencia de la variable seguridad de información de la variable de gestión de riesgo de TI del 44%, por lo que se indica que a una buena gestión de riesgos existe la probabilidad de una eficiente seguridad de la información, pero también está presente la probabilidad de que a una mala gestión de riesgos, la seguridad de la información sea deficiente.

Herrera (2017) en su investigación Digitalización de documentos y seguridad de la información en la Contraloría General de la República - Lima 2016. La problemática de la investigación fue que la Oficina Central de Registros Académicos y Centro de Cómputo (OCRACC), de la Universidad Nacional Federico Villarreal, ente responsable de coordinar y ejecutar las actividades de recopilación, registro, procesamiento de información de matrícula y notas de los estudiantes, y emisión de la documentación académica oficial de los estudiantes y egresados de la Universidad, así también es responsable de los procesos documentarios. El proceso de registro de matrícula y notas suceden en las Facultades y Escuelas Universitarias en un aplicativo de escritorio, y concluido este proceso, la

información es remitida a la OCRACC para su procesamiento según los normas vigentes y calendario académico, observándose demora en envío de la información por parte de las dependencias correspondientes, generando baja disponibilidad de la información para el estudiante o egresado, al ser sensible y de cuidado la información de matrícula, notas y emisión de documentos académicos oficiales, se constituye en una de sus funciones críticas y de alta confianza, respondiendo a la necesidad de mejorar el proceso y nivel de la seguridad de información. La metodología empleada ISO 27001. El tipo de estudio básico nivel descriptivo correlacional, diseño no experimental de corte transversal y enfoque cuantitativo. Población conformada por 55 usuarios (cliente interno) de la Oficina Central de Registros Académicos y Centro de Computo de la Universidad Nacional Federico Villarreal, pertenecientes a las áreas usuarias Instrumento. Como resultado se determinó que existe una relación directa y significativa de nivel moderado entre la seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016, obteniendo como resultado Rho de Spearman = 0.683** y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Vergara (2017) Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016. Se tiene problemas de espacio ocupado por los documentos en físico, altos tiempos de respuesta para la búsqueda de documentos, alto riesgo de pérdida o mutilación de información, particularmente, de eliminarse los documentos históricos, que incluyen informes así como toda la evidencia documental y documentos de trabajo, que por recomendación del Órgano de Control Institucional de la Entidad deben ser eliminados por exceder el tiempo que deben estar almacenados en el archivo central, la falta de normativa orientada y el soporte técnico para la digitalización de documentos, y la cultura organizacional apegada a gestionar los documentos en soporte en papel, generan un problema que impacta en la disponibilidad, integridad y confidencialidad de la información. De ahí que, la entidad requiere la conservación de la información contenida en grandes volúmenes de documentos en soporte en papel. Metodología ISO 27001. Tipo de estudio básica de nivel correlacional, no experimental de corte transversal y enfoque cuantitativo. Población fue 71 trabajadores de la Contraloría General de la República. Y la muestra conformada por 60 personas. El Instrumento fue el Cuestionario.

Carrión (2015) en su investigación Diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM-Huaraz, 2014. Para este diagnóstico de la gestión de riesgo, se basó en la ISO/lEC

27002:2008 y a su vez en la metodología MAGERIT. El tipo de estudio es básica descriptiva simple. Bajo el enfoque cuantitativas y cualitativas. La población conformada por 6274 alumnos, 480 personal docente y 60 personal administrativo, resultado un total de 6814. Mientras que la muestra un total de 624. El instrumento entrevista, observación y encuesta. En conclusión, la mejora de los procesos académicos de la OGE se verá evidenciadas una vez se apliquen las medidas para una apropiada gestión de riesgos, la cual comprende las salvaguardas elegidas, controles establecidos y el plan de seguridad.

Variable Gestión de riesgos, según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Metodología MAGERIT (2012) estableció que, "Hay dos grandes tareas a realizar: I. análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar. II. tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume. Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos" (p. 19). Corda, Viñas y Coria (2017) "Una GRi, idealmente, debería estudiar los riesgos bajo ciertos parámetros y metodologías, para poder predecirlos, prevenirlos o controlarlos y así dejen de ser una incertidumbre y los causantes de muchos obstáculos y malos momentos para nuestras organizaciones" (p. 4).

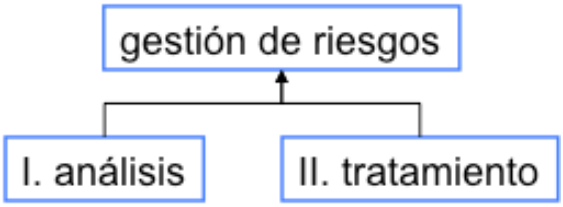


Figura 1. Gestión de riesgos

Tomado de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información", libro I Método, versión 3.0, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Magerit.

Mosoiu, Cioaca y Bălăceanu (2018) "riesgos sistemáticos y riesgos no sistémicos. El primer riesgo se refiere a la variabilidad del ingreso causada por factores externos (condiciones macroeconómicas). El riesgo no sistemático se refiere a los ingresos variabilidad causada por factores impredecibles (decisiones de mala gestión, tecnologías

abruptas superadas)" (p. 1). Seul-Ki, Taejin y Jin (2019) "A medida que la tecnología de las TIC evoluciona, el código malicioso también se vuelve más inteligente y automatizado, lo que representa una amenaza importante para los usuarios de las tecnologías TIC" (p. 3). Para Muhammad (2019) "el agente es la persona que realiza la evaluación preliminar apuntando a los procesos comerciales y objetivos. Identifica y analiza las partes interesadas, identifica los activos afectados por el riesgo, estima su costo de daños, identifica al propietario de los activos, evalúa todos los activos que puede ser objetivo de los riesgos, amenazas y vulnerabilidades" (p. 7).

La metodología MAGERIT, Siguiendo la terminología de la normativa ISO 31000, MAGERIT responde a lo que se denomina "Proceso de Gestión de los Riesgos", sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. (p. 7)

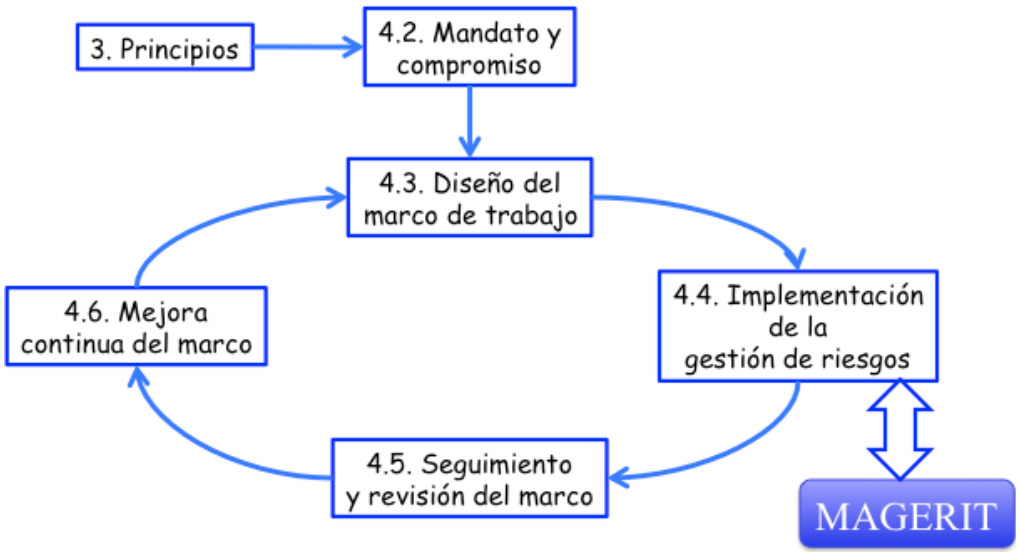


Figura 2. ISO 31000 - Marco de trabajo para la gestión de riesgos

Tomado de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información", libro I Método, versión 3.0, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Magerit.

La metodología MAGERIT divide sus objetivos en dos grandes grupos directos e indirectos: "Directos, se refiere a concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos. Ofrecer un

método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC) Y finalmente, Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. E Indirectos, a preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación. Búsqueda de la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos como es el Modelo de valor, Mapa de riesgos, Declaración de aplicabilidad, Evaluación de salvaguardas, Estado de riesgo, Informe de insuficiencias, Cumplimiento de normativa, Plan de seguridad" (p. 8). Basándome en la primera actividad de la metodología Magerit el Método de análisis de riesgos, se consideró las siguientes dimensiones "Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación. Determinar a qué amenazas están expuestos aquellos activos. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza. Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza" (p. 22).

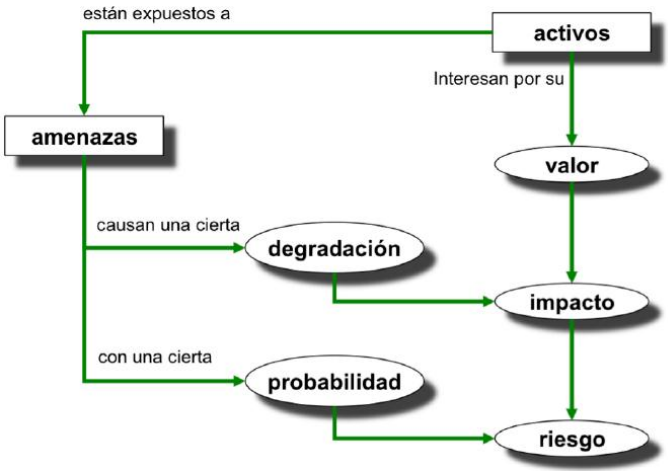


Figura 3. Elementos del análisis de riesgos potenciales

Tomado de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información", libro I Método, versión 3.0, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Magerit.

Dimensión 1: Activos de información, La metodología Magerit (2012) "Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización" (p. 22).

Un activo es superior cuando depende de otro, mientras que el activo inferior cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior. Cuando la materialización de una amenaza en el activo inferior tiene como consecuencia un perjuicio sobre el activo superior. Con frecuencia se puede estructurar el conjunto de activos en capas: Activos esenciales (información que se maneja y servicios prestados), Servicios internos (que estructuran ordenadamente el sistema de información), El equipamiento informático (software, hardware, comunicaciones, soportes de información: discos, cintas, etc.), El entorno: activos que se precisan para garantizar las siguientes capas (equipamiento y suministros: energía, climatización, mobiliario), Los servicios subcontratados a terceros, Las instalaciones físicas y el personal (usuarios, operadores y administradores y desarrolladores.

Para Erceg "La información es el activo más valioso una organización (privado, público, gubernamental, no gubernamental). Es importante desarrollar una combinación de sistemas, operación y procedimientos internos para garantizar la integridad de la organización" (p. 123).

Dimensión 2: Amenazas, La metodología Magerit: "Consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son cosas que ocurren. Y, de todo lo que puede ocurrir, interesa lo que puede pasarles a nuestros activos y causar un daño" (p. 27).

Cinco tipos de identificar las amenazas: 1 De origen natural: Accidentes naturales (terremotos, inundaciones, etc.) Víctima pasiva. 2 Del entorno (de origen industrial): Hay desastres industriales (contaminación, fallos eléctricos, ...) víctima pasiva; pero no por ser pasivos hay que permanecer indefensos. 3 Defectos de las aplicaciones: Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Vulnerabilidades. 4 Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión. 5 Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

Dimensión 3: Determinación de impacto potencial, "Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo

derivar el impacto que estas tendrían sobre el sistema" (p. 28). Impacto acumulado, "es el calculado sobre un activo teniendo en cuenta su valor acumulado (el propio mas el acumulado de los activos que dependen de él) y las amenazas a que está expuesto" (p. 28). Mientras que el Impacto repercutido, "es el calculado sobre un activo teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende" (p. 29).

Dimensión 4: Determinación del riesgo potencial, La metodología Magerit "denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia. El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo: zona 1 (riesgos muy probables y de muy alto impacto), zona 2 (franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo), zona 3 (riesgos improbables y de bajo impacto) y zona 4 (riesgos improbables, pero de muy alto impacto)" (p. 29).

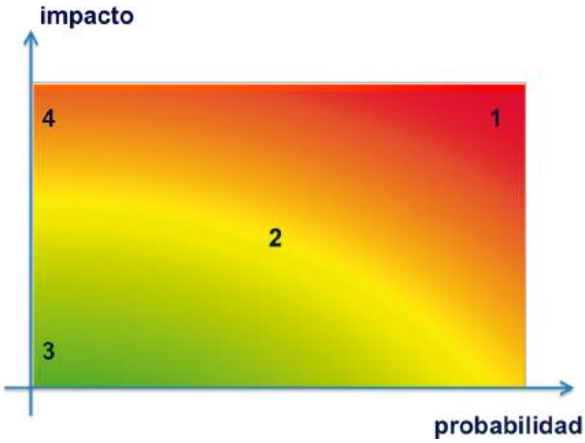


Figura 4. El riesgo en función del impacto y la probabilidad

Tomado de "Metodología de Análisis y Gestión de Riesgos de los sistemas de Información", libro I Método, versión 3.0, 2012. Ministerio de Hacienda y Administraciones Públicas. Madrid, España: Magerit.

Dimensión 5: Salvaguardas, La metodología Magerit define la dimensión salvaguarda como: "contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal" (p. 31).

Variable Seguridad de la información, la NTP-ISO/IEC 17799 (2007) define la seguridad de la información de la siguiente manera: "La información es un activo importante del negocio, tiene valor para la organización y requiere una protección adecuada. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas, puede estar impresa, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información protege de amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. Se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización" (p.7). Youngin, Junhyoung, Sooheon y Kyungho (2018) "Los modelos de gobernanza son similares a los modelos de madurez de seguridad de la información (ISMM). La cual incluye los elementos que la SI de una organización debería considerar para una gestión efectiva. Las mejores prácticas describen que pueden implementarse para reducir costos" (p. 4).

La seguridad de la información, según ISO 27001, "es la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: Confidencialidad (la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados), integridad (mantenimiento de la exactitud y completitud de la información y sus métodos de proceso) y disponibilidad (acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran)" (p. 10). Alemán y Rodríguez "La implementación de un Sistema de Gestión de Seguridad Informática (SGSI) se encuentra determinada por la estructura organizacional de las instituciones, lo que abarca características como: tipo, tamaño, objetivos, servicios, procesos, personal y

requerimientos de seguridad que establece la misma, para lo cual se apoya en estándares internacionales tales como ISO/IEC 27001, norma en la que se describen un conjunto de herramientas corporativas que permiten establecer un plan de acción para la solución de problemas de seguridad a nivel técnico, organizativo y legislativo en una empresa" (p. 1).

Metodología ISO 27001:2014 La Norma Técnica Peruana "ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo" (p. 8). La Norma también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

Dimensión 1: Confidencialidad, para Galindo (2014) "La Segunda Cohorte del Doctorado en Seguridad Estratégica" la define, Característica que no permite la difusión de la información a personal o sistemas que no se encuentren autorizados" (p.165).

Dimensión 2: Integridad, según Galindo (2014) "La Segunda Cohorte del Doctorado en Seguridad Estratégica" la define, es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran" (p. 167).

Dimensión 3: Disponibilidad, según Galindo (2014) La Segunda Cohorte del Doctorado en Seguridad Estratégica la define, como "Característica cuyo objeto es que los datos no sufran alteraciones no autorizadas, por lo cual la información se mantiene tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados" (p.166).

Problema general, ¿Cuál es la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? Y los problemas específicos:

(1) ¿Cuál es la relación entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? (2) ¿Cuál es la relación entre las amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? (3) ¿Cuál es la relación entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? (4) ¿Cuál es la relación entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? (5) ¿Cuál es la relación entre salvaguarda la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019?

Justificación Teórica, esta investigación teóricamente se justifica, pues la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT (2012) respecto a la gestión de riesgos "(…) donde el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados: activos de información, amenazas, impacto potencial, riesgo potencial y salvaguardas (…)" y colabora en con nuestra investigación, ya que por otro lado NTP ISO 27001:2014 (2014) respecto a seguridad de la información "(…) permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma (…)", complementa en el análisis de la eficiencia de la gestión de riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE. Esta investigación buscó, mediante la propuesta de la teoría fue determinar la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019.

Justificación práctica, esta investigación permitió al Programa Fortalece Perú del MTPE, medir la correlación que existe entre la Gestión de Riesgos y la Seguridad de la Información, cuya finalidad es establecer la relación entre la gestión de riesgos y seguridad de la información, para ello se utilizará la metodología MAGERIT para el diagnóstico de la primera variable (Gestión de riesgos), y la metodología ISO 27001 para la segunda variable (seguridad de la información). Permitiendo una mejor toma de decisiones y asegurar la continuidad operativa del Programa.

Metodológicamente se justifica, porque se utilizó una investigación de enfoque cuantitativo y método hipotético deductivo, de tipo básica y de nivel correlacional con un diseño no experimental de corte transversal, que permitió medir la correlación que existe entre la Gestión de Riesgos y la seguridad de la información, donde para la toma de información

se realizó la técnica el cuestionario como instrumento de medición, para medir los activos de información, amenazas, impacto potencial, riesgo potencial y salvaguardas de la gestión de riesgos y la confidencialidad, la integridad y la disponibilidad de la seguridad de la información y su procesamiento en el software SPSS, instrumentos que han sido validados por juicio de expertos y sometidos a la prueba de confiabilidad, y que podrán ser utilizados en posteriores investigaciones en el tema tratado. La población estuvo conformada por los consultores que conforman el Programa Fortalece Perú (25), y la muestra también de 25.

El objetivo general es Determinar la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 y los objetivos específicos: (1) Determinar la relación entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (2) Determinar la relación entre las amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (3) Determinar la relación entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (4) Determinar la relación entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (5) Determinar la relación entre salvaguardar la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019

Hipótesis general Existe una relación directa entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019. Y las hipótesis específicas: (1) Existe una relación directa entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (2) Existe una relación directa entre las amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (3) Existe una relación directa entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (4) Existe una relación directa entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 (5) Existe una relación directa entre salvaguardar la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019

II. Método

2.1. Tipo y diseño de investigación

"La investigación obedece a un diseño no experimental de corte transversal, pues no se desarrolló ningún tratamiento experimental y la recolección de datos se realizó en un solo momento" (Hernández, Fernández y Baptista, 2010, p. 151).

Por otra parte, señalaron que los estudios no experimentales son "investigaciones que se realizan sin la modificación intencionada de variables y que solo se evidencian los sucesos en naturalmente para su posterior análisis". (Hernández, et al., 2010, p. 149).

El estudio es de corte transversal, toda vez que no se modificaron los datos de las variables, gestión de riesgos y seguridad de la información, solo se ha descrito sus propiedades y transcendencia de los mismos, y se realizó en un solo momento la recolección de los datos a los usuarios.

2.2. Operacionalización de variables

Definición conceptual de la variable Gestión de riesgos: La metodología MAGERIT (2012) estableció que, "Hay dos grandes tareas a realizar: I. análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar. II. Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume" (p. 19).

Definición operacional de la variable Gestión de riesgos: La metodología MAGERIT (2012) "El análisis de riesgos considera los siguientes elementos: 1. activos de información, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización. 2. amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización. 3. salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen daño. 4. el impacto potencial: lo que podría pasar. 5. El riesgo potencial: lo que probablemente pase." (p. 19).

Definición conceptual de la variable Seguridad de la información: El ISO 27001 define: "La información es un activo que, como otros activos importantes del

negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades" (p. 1).

Definición operacional de la variable Seguridad de la información

El ISO 27001 define 3 dimensiones importantes "(1) Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (2) Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. (3) Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran" (p. 165-166).

Tabla 1

Matriz de operacionalización de la variable Gestión de riesgos

Dimensiones	**Indicadores**	**Ítems**	**Escala de medición y valores**	**Niveles y rangos**
Activos de información	Activos esenciales	1,2,3	1= Totalmente en desacuerdo 2= En Desacuerdo 3= Indeciso 4= De acuerdo 5= Totalmente de acuerdo	Bajo: 1 - 5 Medio: 6 - 10 Alto: 11 - 15
Amenazas	Identificación amenazas	4,5,6,7,8		Bajo: 1 - 8 Medio: 9-16 Alto: 17 - 25
Impacto Potencial	Impacto acumulado Impacto repercutorio	9 10		Bajo: 1 - 3 Medio: 4 - 6 Alto: 7 - 10
Riesgo potencial	Riesgo acumulado Riesgo repercutido	11 12		Bajo: 1 - 3 Medio: 4 - 6 Alto: 7 - 10

Salvaguardas	Selección salvaguardas Efectos de las salvaguardas	13 14,15,16, 17,18,19, 20,21,22	Bajo: 1 - 16 Medio: 17-32 Alto: 33 - 50

Tomado de Otoya

Tabla 2

Matriz de operacionalización de la variable Seguridad de la información

Dimensiones	**Indicadores**	**Ítems**	**Escala de medición y valores**	**Niveles y rangos**
Confidencialidad	Control de acceso Autentificación Auditable	1,2 3,4 5,6	1= Totalmente en desacuerdo 2= En Desacuerdo	Bajo: 1 - 10 Medio:11-20 Alto:21– 30
Integridad	Seguridad de la comunicación Protección	7,8,9 10	3= Indeciso 4= De acuerdo 5=Totalmente de acuerdo	Bajo: 1 - 7 Medio:8-14 Alto:15– 20
Disponibilidad	Continuidad de la regla del negocio Acceso a la información	11,12 13,14		Bajo:1 - 7 Medio:8-14 Alto:15- 20

Tomado de Vergara Quiroz

2.3. Población y muestra

La población estuvo conformada por 25 colaboradores del Programa Fortalece Perú del Ministerio de Trabajo y Promoción del Empleo.

La muestra, para Hernández "si la población es menor a cincuenta individuos, la población es igual a la muestra" Por tanto, conociendo el tamaño de la población, siendo menor a 25 individuos.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

La técnica de recolección de los datos fue la Encuesta. Vinuesa (2005) la define como "La encuesta es un procedimiento estadístico que permite captar la opinión de una sociedad o de un grupo social para determinar el sentido y la intensidad de las corrientes de opinión mayoritarias. Captan tanto situaciones y hechos como opiniones, y este doble aspecto no debe perderse de vista" (p.177).

El Instrumento de recolección de datos fue el Cuestionario con escala de tipo Likert modificado, como: 1) Totalmente en desacuerdo, 2) En Desacuerdo, 3) Indeciso, 4) De acuerdo y 5) Totalmente de acuerdo. García (2006) lo define, como: "Conjunto ordenado de preguntas en un lenguaje comprensible y natural, que puede o no necesitar la guía de un encuestador se responden normalmente por escrito" (p.29).

Ficha técnica del instrumento 1

Nombre del Instrumento 1: Cuestionario para medir la gestión de riesgos

Autor y año: Lourdes Harumi Calderon Taboada, 2019

Universo de estudio: Consta de 22 interrogantes.

Nivel de confianza: 95.0%

Margen de error: 5.0%

Tamaño muestral: 25

Tipo de técnica: Encuesta

Tipo de instrumento: Cuestionario

Fecha trabajo de campo: 28 de junio de 2019

Escala de medición: 1= Totalmente en desacuerdo, 2= En Desacuerdo, 3= Indeciso, 4= De acuerdo, 5= Totalmente de acuerdo.

Tiempo utilizado: 20 min.

Ficha técnica del instrumento 2

Nombre del Instrumento 2: Cuestionario para medir la seguridad de la información

Autor y año: Lourdes Harumi Calderon Taboada, 2019

Universo de estudio: Consta de 14 interrogantes.

Nivel de confianza: 95.0%

Margen de error: 5.0%

Tamaño muestral: 25

Tipo de técnica: Encuesta

Tipo de instrumento: Cuestionario

Fecha trabajo de campo: 28 de junio de 2019

Escala de medición: 1= Totalmente en desacuerdo, 2= En Desacuerdo, 3= Indeciso, 4= De acuerdo, 5= Totalmente de acuerdo.

Tiempo utilizado: 20 min.

La validez en términos generales, se refiere al grado en que un instrumento realmente mide la variable que pretende medir (Hernández, Fernández y Baptista, 2010). Para la validación de los instrumentos, se sometieron a consideraciones de juicio de expertos. Hernández, Fernández y Baptista (2010), el juicio de expertos (ver anexos 8 y 9) para contrastar la validez de los ítems consiste en preguntar a personas expertas en el dominio que miden los ítems, sobre su grado de adecuación a un criterio determinado y previamente establecido.

Tabla 3.

Juicio de expertos

Experto	El instrumento presenta				Condición Final
	Pertinencia	Relevancia	Claridad	Suficiencia	
Juez 1	Sí	Sí	Sí	Sí	Aplicable
Juez 2	Sí	Sí	Sí	Sí	Aplicable
Juez 3	Sí	Sí	Sí	Sí	Aplicable

Fuente: Validación de instrumentos

Confiabilidad, los instrumentos de recolección de datos que se emplearon en la investigación tiene ítems con opciones en escala Likert, por lo cual se ha utilizado el coeficiente alfa de Cronbach para determinar la consistencia interna, analizando la correlación media de cada ítem con todas las demás que integran dicho instrumento. Para determinar el coeficiente de confiabilidad, se aplicó la prueba piloto, después de analizo mediante el alfa de Cronbach con la ayuda del software estadístico SPSS versión 24. La escala de valores que determina la confiabilidad está dada por los siguientes valores (Escobedo, Mendoza, y Cuervo 2009) Alrededor de 0.9, es un nivel elevado de confiabilidad. La confiabilidad de 0.8 o superior puede ser

considerada como confiable Alrededor de 0.7, se considera baja Inferior a 0.6, indica una confiabilidad inaceptablemente baja.

Tabla 4.

Confiabilidad de instrumentos – Alfa de Cronbach

Instrumento	Alfa de Cronbach	Nª Items
Gestión de riesgos	0.753	22
Seguridad de la información	0.753	14
Promedio	0.753	

De acuerdo a los resultados y teniendo en cuenta el índice de fiabilidad obtenido por el alfa de Cronbach igual a 0.753 y 0.753, se puede asumir que los instrumentos son confiables y procede su aplicación.

2.5. Métodos de análisis de datos

Una vez recolectados los datos de la investigación, se procedió al análisis estadístico respectivo. Los datos fueron tabulados y se presentan las tablas y figuras de distribución de frecuencias. Los datos fueron tabulados en el software estadístico SPSS V 24. Debido a que las variables son cuantitativas, se empleó, para la contratación de las hipótesis la prueba no paramétrica de regresión logarítmica ordinal, que es una medida de causa-efecto para variables que requiere mínimamente de un nivel de medición ordinal, de tal modo que los individuos u objetos de la muestra puedan ordenarse por rangos. El análisis de los datos se realizó con el software estadístico SPSS versión 24.

2.6. Aspectos éticos

La investigación prima en el ejercicio de un acto responsable, motivo por el que la investigación no esconde la naturaleza de la investigación a los contribuyentes, ni comprometer a los contribuyentes en actos perjudiciales, y en absolutos e infringió su intimidad, los datos asignados son reales a su naturaleza y sin alteraciones realizadas por el investigador, no siendo sólo un acto técnico.

III. Resultados

Resultados descriptivos

Tabla 5

Niveles de la variable Gestión de Riesgos del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	7	28,0	28,0	28,0
	Medio	5	20,0	20,0	48,0
	Alto	13	52,0	52,0	100,0
	Total	25	100,0	100,0	

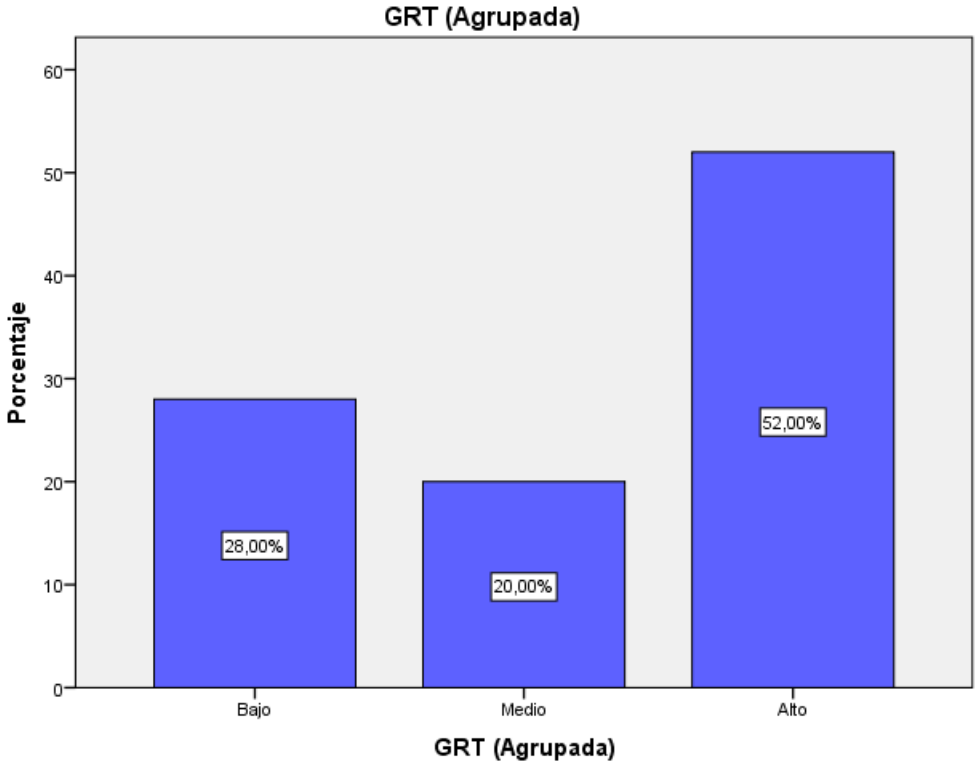


Figura 5: Niveles de la variable Gestión de Riesgos del Programa Fortalece Perú

En la tabla 5 y figura 5, donde se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 28% (7) consideran medio, 20% (5) consideran medio y 52% (13) consideran alto.

Tabla 6

Niveles de la variable Gestión de Riesgos – Dimensión Activos de Información del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	14	56,0	56,0	56,0
	Medio	10	40,0	40,0	96,0
	Alto	1	4,0	4,0	100,0
	Total	25	100,0	100,0	

En la tabla 6, se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 56% (14) consideran medio, 40% (10) consideran medio y 4% (1) consideran alto.

Tabla 7

Niveles de la variable Gestión de Riesgos – Dimensión Amenazas del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	5	20,0	20,0	20,0
	Medio	10	40,0	40,0	60,0
	Alto	10	40,0	40,0	100,0
	Total	25	100,0	100,0	

En la tabla 7, se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 20% (5) consideran medio, 40% (10) consideran medio y 40% (10) consideran alto.

Tabla 8

Niveles de la variable Gestión de Riesgos – Dimensión Impacto potencial del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	12,0	12,0	12,0
	Medio	13	52,0	52,0	64,0
	Alto	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

En la tabla 8, se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 12% (3) consideran medio, 52% (13) consideran medio y 36% (9) consideran alto.

Tabla 9

Niveles de la variable Gestión de Riesgos – Dimensión Riesgo potencial del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	3	12,0	12,0	12,0
	Medio	13	52,0	52,0	64,0
	Alto	9	36,0	36,0	100,0
	Total	25	100,0	100,0	

En la tabla 9, se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 12% (3) consideran medio, 52% (13) consideran medio y 36% (9) consideran alto.

Tabla 10

Niveles de la variable Gestión de Riesgos – Dimensión Salvaguardas del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	44,0	44,0	44,0
	Medio	3	12,0	12,0	56,0
	Alto	11	44,0	44,0	100,0
	Total	25	100,0	100,0	

En la tabla 10, se muestran los porcentajes de la variable 1 Gestión de Riesgos (V1), donde podemos interpretar que un 44% (11) consideran medio, 12% (3) consideran medio y 44% (11) consideran alto.

Tabla 11

Niveles de la variable Gestión de Riesgos del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	12	48,0	48,0	48,0
	Medio	10	40,0	40,0	88,0
	Alto	3	12,0	12,0	100,0
	Total	25	100,0	100,0	

En la tabla 11, se muestran los porcentajes de la variable 1 Seguridad de la Información (V2), donde podemos interpretar que un 48% (12) consideran medio, 40% (10) consideran medio y 12% (3) consideran alto.

Tabla 12

Niveles de la variable Seguridad de la Información – Dimensión Confiabilidad del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	44,0	44,0	44,0
	Medio	10	40,0	40,0	84,0
	Alto	4	16,0	16,0	100,0
	Total	25	100,0	100,0	

n la tabla 12, se muestran los porcentajes de la variable 2 Seguridad de la Información (V2), donde podemos interpretar que un 44% (11) consideran medio, 40% (10) consideran medio y 16% (4) consideran alto.

Tabla 13

Niveles de la variable Seguridad de la Información – Dimensión Integridad del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	11	44,0	44,0	44,0
	Medio	11	44,0	44,0	88,0
	Alto	3	12,0	12,0	100,0
	Total	25	100,0	100,0	

En la tabla 13, se muestran los porcentajes de la variable 2 Seguridad de la Información (V2), donde podemos interpretar que un 44% (11) consideran medio, 44% (11) consideran medio y 12% (3) consideran alto.

Tabla 14

Niveles de la variable Seguridad de la Información – Dimensión Disponibilidad del Programa Fortalece Perú

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	15	60,0	60,0	60,0
	Medio	7	28,0	28,0	88,0
	Alto	3	12,0	12,0	100,0
	Total	25	100,0	100,0	

En la tabla 14, se muestran los porcentajes de la variable 2 Gestión de Riesgos (V2), donde podemos interpretar que un 60% (15) consideran medio, 28% (7) consideran medio y 12% (3) consideran alto.

Prueba de hipótesis general

Ho: No existe una relación directa entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019.

Ha: Existe una relación directa entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019.

Tabla 15

Correlación No paramétrica relación Gestión de Riesgos y Seguridad de la Información

Correlaciones

			GRT (Agrupada)	SIT (Agrupada)
Rho de Spearman	GRT (Agrupada)	Coeficiente de correlación	1,000	,661**
		Sig. (bilateral)	.	,000
		N	25	25
	SIT (Agrupada)	Coeficiente de correlación	,661**	1,000
		Sig. (bilateral)	,000	.
		N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El resultado sig (bilateral) es de 0,000 o 0,00% el cual es menor a 0,01 o 1% y se obtiene un coeficiente de correlación de 0.661, lo cual indica que existe relación entre las variables.

Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna; se concluye que, Existe relación directa entre Gestión de riesgos y Seguridad de la información en el Programa Fortalece Perú del MTPE, 2019.

Prueba de hipótesis específicas

Prueba de hipótesis específica 1

Ho: No existe una relación directa entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019.

Ha: Existe una relación directa entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019.

Tabla 16

Correlación No paramétrica relación Activos de información y Seguridad de la Información

Correlaciones

			GRAIT (Agrupada)	SIT (Agrupada)
Rho de Spearman	GRAIT (Agrupada)	Coeficiente de correlación	1,000	,658**
		Sig. (bilateral)	.	,000
		N	25	25
	SIT (Agrupada)	Coeficiente de correlación	,658**	1,000
		Sig. (bilateral)	,000	.
		N	25	25

**. La correlación es significativa en el nivel 0,01 (bilateral).

El resultado sig (bilateral) es de 0,000 o 0,00% el cual es menor a 0,01 o 1% y se obtiene un coeficiente de correlación de 0.658, lo cual indica que existe relación entre las variables. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna; se concluye que, Existe relación directa entre Activos de información y Seguridad de la información en el Programa Fortalece Perú del MTPE, 2019.

IV. Discusión

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 5, en donde el 28% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 20% percibe que el nivel es medio y el 52% percibe que el nivel de la gestión de riesgos en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es medio.

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 6, en donde el 56% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 40% percibe que el nivel es medio y el 4% percibe que el nivel de los activos de información en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es bajo.

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 7, en donde el 20% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 40% percibe que el nivel es medio y el 40% percibe que el nivel de la amenaza en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es medio.

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 8, en donde el 12% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 52% percibe que el nivel es medio y el 36% percibe que el nivel del impacto potencial en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es medio.

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 9, en donde el 12% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 52% percibe que el nivel es medio y el 36% percibe que el nivel del riesgo potencial en el Programa Fortalece Perú es alto. Lo que

evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es medio.

Los resultados generales de la seguridad de la información en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 10, en donde el 44% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 12% percibe que el nivel es medio y el 44% percibe que el nivel de salvaguardas en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es bajo.

Los resultados generales de la gestión de riesgos en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 11, en donde el 48% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 40% percibe que el nivel es medio y el 12% percibe que el nivel de integridad en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es bajo.

Los resultados generales de la gestión de riesgos en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 12, en donde el 44% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 40% percibe que el nivel es medio y el 16% percibe que el nivel de confidencialidad en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es bajo.

Los resultados generales de la gestión de riesgos en el Programa Fortalece Perú 2019, tal como se aprecia en la tabla 13, en donde el 44% percibe que el nivel es bajo en cuanto a la gestión de riesgos, mientras que el 44% percibe que el nivel es medio y el 12% percibe que el nivel de disponibilidad en el Programa Fortalece Perú es alto. Lo que evidencia que el nivel de la seguridad de la información en el Programa Fortalece Perú es bajo.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual de la gestión de riesgos en la seguridad de la información en un 66%.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual de los activos de información en la seguridad de la información en un 65,8%.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual de las amenazasen la seguridad de la información en un 67,5%.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual del impacto potencial en la seguridad de la información en un 40,5%.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual de riesgo potencial en la seguridad de la información en un 40,5%.

En la prueba de hipótesis general se rechaza la hipótesis nula como se observa en la tabla 15, presentando la dependencia porcentual de salvaguardas en la seguridad de la información en un 61,5%.

V. Conclusiones

Primera conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre la gestión de riesgos y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.661 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Segunda conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre la los activos de información y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.658 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Tercera conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre la los amenazas y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.675 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Cuarta conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre el impacto potencial y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.405 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Quinta conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre el riesgo potencial y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.405 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

Sexta conclusión

Se ha determinado que existe una relación directa y significativa de nivel medio entre salvaguardas y la seguridad de la información del Programa Fortalece Perú 2019, obteniendo como resultado Rho de Spearman = 0.615 y un p-valor =0.000<0.05, en tal sentido se comprobó la hipótesis alterna y se rechaza la hipótesis nula.

VI. Recomendaciones

Primera:

Se propone implementar la gestión del riesgo tiendo en cuenta sus dos actividades (análisis de riesgos y el tratamiento). Por lo que es necesario tener en cuenta para esta implementación una adecuada administración de activos de información, identificar sus amenazas, minimizar la ejecución del riesgo y su impacto potencial; así como la adecuada aplicación de salvaguardas al riesgo.

Segunda:

Se propone implementar la gestión de riesgos en el Programa Fortalece Perú, utilizando la metodología Margerit.

Tercera:

Se propone implementar el sistema de gestión de seguridad de información (SGSI) en el Programa Fortalece Perú, utilizando la metodología Magerit acoplada a la norma técnica peruana NTP - ISO/ IEC 27001: 2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de seguridad de la información. Requisitos (Segunda ed.)

Cuarta:

Realizar seguimiento y control permanente de acuerdo a la gestión del cambio a las implementaciones de administración de riesgos y al sistema de gestión de seguridad de la información.

Referencias

Aguilera Almaguer, O, Pérez Alí, E y Rivero Cuesta, R. (2017) *La protección de la información. Una visión desde las entidades educativas cubanas.* Cuba.

Alemán Novoa, H. & Rodríguez Barrera, C. (2015). Metodologías para el análisis de riesgos en los sgsi. 9(0). 73-86. DOI 10.22490/25394088.1435

Arévalo Ascanio, J. G., Bayona Trillos, R. A., Rico Bautista, D. W. (2015). Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. *Implantation of a safety management system information under the ISO 27001: risk analysis information. Vol. 19 Issue 46,* p123-134. 12p. DOI: 10.14483/udistrital.jour.tecnura.2015.4.a10

Barlow, J. B., Warkentin, M., Ormond, D. & Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. *Journal of the Association for Information Systems Vol. 19* Issue 8, p689-715. 27p. DOI: 10.17705/1jais.00506

Boateng, K. A., Coffie, R. B. & Hayford, P. (2018). Trust in the Public Sector? On Information Security Awareness in an Audit Service. *Journal of Information Technology & Economic Development, Vol. 9 Issue 1*, p23-37. 15p

Carol, H., Jae Nam, L. & Straub, D. W. (2012). *Institutional Influences on Information Systems Security Innovations. Information Systems Research, Vol. 23 Issue 3*, p918-939. 22p. DOI: 10.1287/isre.1110.0393

Carrión Apéstegui, S. (2015) *Diagnóstico y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27002:2008 para la oficina general de estudios UNASAM-Huaraz, 2014.* (Tesis de título inédita). Universidad Nacional Santiago Antúnez de Mayolo.

Chad, A., Baskerville, R. L. & Kaul, M. (2017). Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the

Privacy of Information. *Journal of Management Information Systems. Vol. 34 Issue 4*, p1082-1112. 31p. DOI: 10.1080/07421222.2017.1394063

Chatterjee, S., Sarker, S. & Valacich, J. S. (2015). The Behavioral Roots of Information Systems Security: Exploring Key Factors Related to Unethical IT Use. *Journal of Management Information Systems, Vol. 31 Issue 4*, p49-87. 39p. DOI: 10.1080/07421222.2014.1001257

Cram, W. A., D'Arcy, J. & Proudfoot, J.G. (2019). Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. *Vol. 43 Issue 2*, p525-554. 54p. DOI: 10.25300/MISQ/2019/15117

Crespo E., Carvajal, F., Astudillo, C., Orellana, M., Vintimilla, R., y Carvallo, J. P. (2018) Acometer contra un ERP con Software Libre. *Vol 9*. 9(1):138-148 DOI 10.29019

Corda, M. C., Viñas, M. & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Technological risk management: transdisciplinary perspective to think about the libraries, Vol. 7 Issue 1*, p1-18. 18p. DOI: 10.24215/18539912e032

Erceg, A. (2019). Information Security: Threat from Employees. *Technical Journal / Tehnicki Glasnik. Vol. 13 Issue 2*, p123-128. 6p. DOI: 10.31803/tg-20180717222848

Fernández Maute, Rubén y Monteros Montenegro, Nelson. (2014) *Propuesta metodológica para la gestión de riesgos tecnológicos en empresas proveedoras de servicios de telecomunicaciones.* (Tesis de maestría inédita). Sangolqui, Ecuador.

Galindo, C. (2014). Seguridad de la Información: Revista de la Segunda Cohorte del Doctorado en Seguridad Estratégica. Guatemala: Universidad San Carlos de Guatemala.

Georg, L. (2017). Information security governance: pending legal responsibilities of non-executive boards. *Journal of Management & Governance, Vol. 21 Issue 4*, p793-814. 22p. DOI: 10.1007/s10997-016-9358

Guevara Chumán, J. (2015) *Aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo*. (Tesis de título inédita). Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Perú.

Hadlington, L. & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *CyberPsychology, Behavior & Social Networking, Vol. 20 Issue 9,* p567-571. 5p. 3 Charts. DOI: 10.1089/cyber.2017.0239

Hernández Sampieri,, R., Fernández Collado, C., & Baptista Lucio, P. (2010). Metodología de la Investigación. McGraw-Hill / Interamericana.

Herrera Castellanos, Erick. (2017) *Digitalización de documentos y seguridad de la información en la Contraloría General de la República - Lima 2016* (Tesis de maestría inédita). Universidad César Vallejo, Lima, Perú.

Hu, Q., West, R. & Smarandescu, L. (2015). The Role of Self-Control in Information Security Violations: Insights from a Cognitive Neuroscience Perspective. *Journal of Management Information Systems. Vol. 31 Issue 4,* p6-48. 43p. 2. DOI: 10.1080/07421222.2014.1001255

Kobek, L. P. & Caldera, E. (2016). Cyber Security and Habeas Data: The Latin American Response to Information Security and Data Protection. *Ciberseguridad y Habeas Data: la respuesta latinoamericana a la seguridad informática y la protección de datos*. *OASIS - Observatorio de Análisis de los Sistemas Internacionales, Issue 24,* p109-128. 20p. DOI: 10.18601/16577558.n24.07

Li, Z. & Wang, J. (2019). Security Storage of Sensitive Information in Cloud Computing Data Center. *International Journal of Performability Engineering. Vol. 15 Issue 3*, p1023-1032. 10p. DOI: 10.23940/ijpe.19.03.p32.10231032

Mäntykangas, A. (2018). Information Security Issues in Higher Education. *eLearning & Software for Education. Vol. 4*, p378-381, 4p; DOI: 10.12753/2066-026X-18-267

Magerit (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro I Método - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro II Catálogo de Elementos - versión 3.0. Madrid, España: Ministerio de Hacienda y Administraciones Públicas.

Magerit. (2012). Metodología de Análisis y Gestión de Riesgos de los sistemas de Información, Libro III Guía de Técnicas - versión 3.0. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Magiort, M. L. (2014). *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información Integrada en los Procesos de Negocio*. (Tesis de maestría inédita). Universidad de Buenos Aires. Argentina.

Martelo, R. J., Madera, J. E. & Betín, A. D. (2015) Software para Gestión Documental, un Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Software for Document Management, a Modular Component of the Information Security Management System (ISMS). Información Tecnológica, Vol. 26 Issue 2,* p129-134. 6p. DOI: 10.4067/S0718-07642015000200015

Martínez Moreno, J., Martínez Moreno, O. A., Mud Castelló, S., Mud Castelló, F., Moreno, L. y Martínez, O. (2015) Análisis de la calidad y seguridad de la información de aplicaciones móviles en prevención terciaria. *Farmacéuticos Comunitarios Vol 7.* 7(4):23-26 DOI: 10.5672/FC.2173-9218

Miloslavskaya, N., Lima, S. & Rocha, A. (2018). Information security management in SOCs and SICs. *Journal of Intelligent & Fuzzy Systems. Vol. 35 Issue 3*, p2637-2647. 11p. DOI: 10.3233/JIFS-169615

Mina Calderón, L. (2015) *Auditoria de seguridad de la información e infraestructura de ti, al área de ti de la empresa de energía de ARAUCA ENELAR E.S.P. del departamento de Arauca.* (Tesis de título inédita). Universidad Cooperativa de Colombia.

Mitkovskiy, A., Ponomarev, A. & Proletarskiy, A. (2019). SIEM-Platform for Research and Educational Tasks on Processing of Security Information Events. *Vol. 3*, p48-56, 9p. DOI: 10.12753/2066-026X-19-143

Molina Miranda, M. (2015). *Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral*. (Tesis de maestría inédita). Universidad Politécnica de Madrid.

Molina Miranda, M. F. (2017). Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. 1(11). DOI 10.31876/re.v1i11.125

Mosoiu, O., Cioaca, C. & Bălăceanu, I. (2018). Using the Capital Asset Pricing Model in Information Security Investments. *eLearning & Software for Education , Vol. 4*, p39-46, 8p; DOI: 10.12753/2066-026X-18-220

Muhammad Imran, T. (2019) Agent Based Information Security Framework for Hybrid Cloud Computing. *KSII Transactions on Internet & Information Systems.* Jan2019, *Vol. 13 Issue 1*, p406-434. 29p. DOI: 10.3837/tiis.2019.01.023

Norma ISO 27001 (Organización Internacional de Estándares). (2013). Sistema de Gestión de Seguridad de Información (SGSI). www.ISO27000.ES

Otoya Verástegui, M. (2018). *Gestión de riesgos de TI en la seguridad de la información del Programa de Desarrollo Productivo Agrario Rural 2017*. (Tesis de maestría inédita). Universidad César Vallejo, Lima, Perú.

Romeral, Luis y Torres Gallego, Álvaro. (2018) *Gestión de Riesgos tecnológicos*. Madrid.

Seul, K, Ch., Taejin, L. & Jin, K. (2019). A Study on Analysis of Malicious Code Behavior Information for Predicting Security Threats in New Environments. *KSII Transactions on Internet & Information Systems, Vol. 13 Issue 3,* p1611-1625. 15p. DOI: 10.3837/tiis.2019.03.028

Singh, V. & Margam, M. (2018). Information Security Measures of Libraries of Central Universities of Delhi : A Study. *DESIDOC Journal of Library & Information Technology. Vol. 38 Issue 2,* p102-109. 8p. DOI: 10.14429/djlit.38.2.11879

Tola Franco, Diana. (2015) *Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001*. (Tesis de título inédita). Escuela Superior Politécnica del Litoral. Guayaquil, Ecuador.

Vergara Quiroz, Gladis. (2017) *Seguridad de información y calidad de servicio en la Universidad Nacional Federico Villarreal, 2016.* (Tesis de maestría inédita). Universidad César Vallejo, Lima, Perú.

Wang, J., Shan, Z., Manish, G. & Raghav, R. H. (2019). A longitudinal study of unauthorized access attempts on information systems: the role of opportunity contexts. *Mis Quarterly. Vol. 43 Issue 2,* p601-622. 30p. DOI: 10.25300/MISQ/2019/14751

Youngin Y., Junhyoung O., Sooheon K. & Kyungho L. (2018). Advanced approach to information security management system utilizing maturity models in critical infrastructure. *KSII Transactions on Internet & Information Systems, Vol. 12 Issue 10,* p4995-5014. 20p. DOI: 10.3837/tiis.2018.10.020

Zhang, X. & Yang, H. (2018). Impact of Cross-Culture on Behavioral Information Security.*Journal of Integrated Design & Process Science, Vol. 22 Issue 2,* p63-80. 18p. DOI: 10.3233/jid-2018-0003

Anexos

Anexo 1: Consentimiento por la institución

Anexo 2: Matriz de Consistencia

Anexo 3: Instrumento de medición de la variable Gestión de riesgos

Anexo 4: Instrumento de medición de la variable Seguridad de la Información

Anexo 5: Certificado de validez de los instrumentos de la variable Gestión de riesgos

Anexo 6: Certificado de validez de los instrumentos de la variable Seguridad de la Información

Anexo 7: Matriz de datos

Anexo 8: Tablas y gráficos alternos del capítulo resultados

Anexo 9: Propuesta de mejora

Anexo 1: Consentimiento por la institución

PERÚ | Ministerio de Trabajo y Promoción del Empleo

"Decenio de la Igualdad de oportunidades para mujeres y hombres"
"Año del Diálogo y la Reconciliación Nacional"

CONSTANCIA

DOMINGO GUZMAN LEON MALVAS
Jefe (e) de la Unidad de Planificación y Presupuesto y Sistemas
Programa Fortalece Perú - MTPE

HACE CONSTAR:

Que, la Srta. Lourdes Harumi Calderón Taboada, identificada con DNI N° 47650978, de profesión Ingeniera de Sistemas, se le otorgó las facilidades para la realización de su investigación sobre Gestión de Riesgos y Seguridad de la Información del Programa Fortalece Perú del MTPE.

Se expide el presente documento a solicitud de la interesada, para los fines que estime conveniente.

Lima, 20 de noviembre del 2018

Unidad de Planificación y Presupuesto y Sistemas
PROGRAMA "FORTALECE PERÚ"

DOMINGO GUZMAN LEON MALVAS
Jefe (e) de la Unidad de Planificación y Presupuesto y Sistemas

Anexo 2: Matriz de Consistencia

<table>
<tr><td colspan="6">Matriz de Consistencia

Título : Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019
Autor : Lourdes Harumi Calderón Taboada</td></tr>
<tr><td>Problema</td><td>Objetivos</td><td>Hipótesis</td><td colspan="3">Variables e indicadores</td></tr>
<tr><td rowspan="4">Problema General:
¿Cuál es la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019?</td><td rowspan="4">Objetivo general:
Determinar la relación entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019</td><td rowspan="4">Hipótesis general:
Existe una relación directa entre la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019</td><td colspan="3">Variable 1: Gestión de riesgos</td></tr>
<tr><td>Dimensiones</td><td>Indicadores</td><td>Ítems</td><td>Escala de medición</td><td>Niveles o rangos</td></tr>
<tr><td>Activos de información</td><td>Activos esenciales</td><td>1,2,3</td><td rowspan="2">1= Totalmente en desacuerdo
2= En Desacuerdo
3= Indeciso
4= De acuerdo</td><td>Bajo:
1 - 5
Medio:
6 - 10
Alto:
11 - 15</td></tr>
<tr><td>Amenazas</td><td>Identificación amenazas</td><td>4,5,6,7,8</td><td>Bajo:
1 - 8
Medio:</td></tr>
</table>

						5=Totalmente de acuerdo	9 – 16 Alto: 17 - 25
Problemas específicos ¿Cuál es la relación entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019?	**Objetivos Específicos** Determinar la relación entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019	**Hipótesis específicas.** Existe una relación directa entre los activos de información la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019	**Impacto potencial**	Impacto acumulado Impacto repercutorio	9 10		Bajo: 1 - 3 Medio: 4 - 6 Alto: 7 - 10
			Riesgo potencial	Riesgo acumulado Riesgo repercutido	11 12		Bajo: 1 - 3 Medio: 4 - 6 Alto: 7 - 10
¿Cuál es la relación entre las	Determinar la relación entre	Existe una relación directa	**Salvaguardas**	Selección salvaguardas Efectos de las salvaguardas	13 14,15,16,17,18,19,20,21, 22		Bajo: 1 - 16 Medio:

amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? ¿Cuál es la relación entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú	las amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 Determinar la relación entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019	entre las amenazas de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 Existe una relación directa entre el impacto potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019					17 - 32 Alto: 33 - 50
			Variable 2: seguridad de la información				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de valores**	**Niveles o rangos**
			Confidencialidad	-Control de Acceso -Autenticación -Auditable	1,2 3,4 5,6	1= Totalmente en desacuerdo 2= En Desacuerdo 3= Indeciso 4= De acuerdo 5=Totalmente de acuerdo	Bajo: 1 - 10 Medio: 11 - 20 Alto: 21 - 30
			Integridad	-Seguridad de la comunicación -Protección	7,8,9 10		Bajo: 1 - 7 Medio: 8 - 14

del MTPE, 2019? ¿Cuál es la relación entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019? ¿Cuál es la relación entre salvaguarda la Gestión de Riesgos y la	Determinar la relación entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 Determinar la relación entre salvaguardar la Gestión de Riesgos y la seguridad de la información del	Existe una relación directa entre el riesgo potencial de la Gestión de Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019 Existe una relación directa entre salvaguardar la Gestión de					Alto: 15 - 20
			Disponibilidad	-Continuidad de la regla del negocio -Acceso a la información	11,12 13,14		Bajo: 1 - 7 Medio: 8 - 14 Alto: 15 - 20

seguridad de la información del Programa Fortalece Perú del MTPE, 2019?	Programa Fortalece Perú del MTPE, 2019	Riesgos y la seguridad de la información del Programa Fortalece Perú del MTPE, 2019					
Tipo y diseño de investigación	**Población y muestra**	**Técnicas e instrumentos**		**Estadística a utilizar**			
Método: Hipotético deductivo **Enfoque:** cuantitativo **Tipo:** Básica **Nivel:** Correlacional **Análisis:** Causa - Efecto	**Población:** 25 consultores del Programa Fortalece Perú-MTPE, 2019 **N :** 25 consultores	**Variable 1: Gestión de riesgos** **Variable 2: seguridad de la información** **Técnicas:** cuestionario **Instrumentos: Ficha de observación**		**DESCRIPTIVA:** Para el análisis estadístico respectivo, se utilizará el paquete estadístico SPSS Versión 22 con licencia de la UCV. Los datos obtenidos serán presentados en tablas y gráficos de acuerdo a las variables y dimensiones, para luego analizarlo e interpretarlos considerando el marco teórico.			

Diseño: No experimental Corte transaccional **Alcance:** La investigación se realizó en el Programa Fortalece Perú del MTPE, ubicado en Jesús María, Lima, Perú.	**Autor:** Lourdes Harumi Calderón Taboada **Tipo de muestreo:** Aleatorio simple **Tamaño de muestra:** n : 25	Autor: Lourdes Harumi Calderon Taboada Año: 2019 Monitoreo: Lourdes Harumi Calderon Taboada Ámbito de Aplicación: Unidad de UPPS de Fortalece Perú - MTPE	**INFERENCIAL:** En base a los instrumentos de recolección de datos tenemos que la variable es cualtitativa ordinal en ese sentido, Para la prueba de hipótesis se aplicará la prueba de la estadística no paramétrica Rho de Spearman con un ($\alpha = 0.05$), el cual se realiza para variables cualitativas ordinales, con la finalidad de inferir los resultados dentro de lo que circunscribirá este estudio. Para Suarez (2013), La inferencia estadística, consiste en llegar a obtener conclusiones o generalizaciones que sobrepasan los límites de los conocimientos aportados por un conjunto de datos. Busca obtener información sobre la población basándose en el estudio de los datos de una muestra tomada a partir de ella (p. 67).

Anexo 3: Instrumento de medición de la variable Gestión de riesgos

Cuestionario para colaboradores de Fortalece Perú del Ministerio de Trabajo
Variable (1): Gestión de riesgos

I. Instrucciones

Estimado(a) colaboradores de Fortalece Perú, el presente instrumento tiene la finalidad de recoger información sobre la gestión de riesgos de TI del Programa Fortalece Perú del Ministerio de Trabajo. Le pedimos que sea sincero en sus respuestas.

II. Información específica

Estimado colaborador, marque sólo una de las opciones:

Totalmente en desacuerdo	En Desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

N°	Ítems	1	2	3	4	5
1	Existe un inventario de activos de información de la información esencial que maneja					
2	Se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja					
3	El equipamiento informático depende del software, hardware, comunicaciones , soporte de información identificados en el inventario de activos de información de TI					
4	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)					

5	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)					
6	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones					
7	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental					
8	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada					
9	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.					
10	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende					
11	Se ha calculado el riesgo acumulado por cada activo de información					
12	Se ha calculado el riesgo repercutido por cada activo de información					
13	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo					
14	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)					
15	Existe un salvaguardas de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)					
16	Existe un salvaguardas de tipo correctiva (gestión de incidentes)					
17	Existe un salvaguardas de tipo recuperación (copias de seguridad backup)					
18	Existe un salvaguardas de tipo monitorización (registros de descargas de la web)					

19	Existe un salvaguardas de tipo detección (antivirus, detectores de incendios, etc.)					
20	Existe un salvaguardas de tipo concientización (cursos de concientización, cursos de formación, etc.)					
21	Existe un salvaguardas de tipo administración (inventario de activos, plan de continuidad)					
22	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales					

Anexo 4: Instrumento de medición de la variable Seguridad de la Información

Cuestionario para colaboradores de Fortalece Perú del Ministerio de Trabajo
Variable (2): Seguridad de la Información

I. Instrucciones

Estimado(a) colaboradores de Fortalece Perú, el presente instrumento tiene la finalidad de recoger información sobre la Seguridad de la nformación de TI del Programa Fortalece Perú del Ministerio de Trabajo. Le pedimos que sea sincero en sus respuestas.

II. Información específica

Estimado colaborador, marque sólo una de las opciones:

Totalmente en desacuerdo	En Desacuerdo	Indeciso	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

N°	**Ítems**	**1**	**2**	**3**	**4**	**5**
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información					
2	Se cuenta con un adecuado inventario de los accesos a los sistemas					
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)					
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios					
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información					

6	Se manejan procedimientos para la autorización formal de solicitudes de accesos					
7	Cuentan con políticas de intercambio de información ya sea física o electrónica					
8	Generan copias de seguridad en la nube de la información propia de la empresa					
9	Realizan controles en la red					
10	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales					
11	Existe un plan de contingencia contra desastres que pongan en riesgo la información					
12	Cuentan con políticas de restauración segura de backups de información					
13	Se cuenta con Directivas o procedimientos para acceder a la información					
14	Existen restricciones para disponer de la información					

Anexo 5: Certificado de validez de los instrumentos de la variable Gestión de riesgos

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. ACTIVOS DE INFORMACIÓN	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existe un inventario de activos de información de la información esencial que maneja							
2	Se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja							
3	El equipamiento informático depende del software, hardware, comunicaciones , soporte de información identificados en el inventario de activos de información de TI							
	II. AMENAZAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
4	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)							
5	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)							
6	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones							
7	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental							
8	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada							

	III. IMPACTO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
9	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.							
10	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende							
	IV. RIESGO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Se ha calculado el riesgo acumulado por cada activo de información							
12	Se ha calculado el riesgo repercutido por cada activo de información							
	V. SALVAGUARDAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
13	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo							
14	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)							
15	Existe un salvaguardas de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)							
16	Existe un salvaguardas de tipo correctiva (gestión de incidentes)							

17	Existe un salvaguardas de tipo recuperación (copias de seguridad backup)							
18	Existe un salvaguardas de tipo monitorización (registros de descargas de la web)							
19	Existe un salvaguardas de tipo detección (antivirus, detectores de incendios, etc.)							
20	Existe un salvaguardas de tipo concientización (cursos de concientización, cursos de formación, etc.)							
21	Existe un salvaguardas de tipo administración (inventario de activos, plan de continuidad)							
22	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales							

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: …….…….……DNI:…….

Especialidad del validador:…….……..

1Pertinencia: El ítem corresponde al concepto teórico formulado.

2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

…….de……..del 20…..

_____

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. ACTIVOS DE INFORMACIÓN	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existe un inventario de activos de información de la información esencial que maneja	✓		✓		✓		
2	Se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja	✓		✓		✓		
3	El equipamiento informático depende del software, hardware, comunicaciones , soporte de información identificados en el inventario de activos de información de TI	✓		✓		✓		
	II. AMENAZAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
4	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	✓		✓		✓		
5	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	✓		✓		✓		
6	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	✓		✓		✓		
7	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	✓		✓		✓		
	III.IMPACTO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	

9	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	✓		✓		✓		
10	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende	✓		✓		✓		
	IV. RIESGO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Se ha calculado el riesgo acumulado por cada activo de información	✓		✓		✓		
12	Se ha calculado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
13	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	✓		✓		✓		
14	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	✓		✓		✓		
15	Existe un salvaguardas de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	✓		✓		✓		
16	Existe un salvaguardas de tipo correctiva (gestión de incidentes)	✓		✓		✓		
17	Existe un salvaguardas de tipo recuperación (copias de seguridad backup)	✓		✓		✓		
18	Existe un salvaguardas de tipo monitorización (registros de descargas de la web)	✓		✓		✓		

19	Existe un salvaguardas de tipo detección (antivirus, detectores de incendios, etc.)	✓		✓		✓		
20	Existe un salvaguardas de tipo concientización (cursos de concientización, cursos de formación, etc.)	✓		✓		✓		
21	Existe un salvaguardas de tipo administración (inventario de activos, plan de continuidad)	✓		✓		✓		
22	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia):

Sí hay

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: ..... **DNI:** 40043433

Especialidad del validador: Dr. en Investigación

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de junio del 2019

Firma del Experto Informante

UCV
UNIVERSIDAD CESAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. ACTIVOS DE INFORMACIÓN	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existe un inventario de activos de información de la información esencial que maneja	✓		✓		✓		
2	Se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja	✓		✓		✓		
3	El equipamiento informático depende del software, hardware, comunicaciones , soporte de información identificados en el inventario de activos de información de TI	✓		✓		✓		
	II. AMENAZAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
4	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	✓		✓		✓		
5	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	✓		✓		✓		
6	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	✓		✓		✓		
7	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	✓		✓		✓		
	III.IMPACTO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	

9	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	✓		✓		✓		
10	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende	✓		✓		✓		
	IV. RIESGO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Se ha calculado el riesgo acumulado por cada activo de información	✓		✓		✓		
12	Se ha calculado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
13	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	✓		✓		✓		
14	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	✓		✓		✓		
15	Existe un salvaguardas de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	✓		✓		✓		
16	Existe un salvaguardas de tipo correctiva (gestión de incidentes)	✓		✓		✓		
17	Existe un salvaguardas de tipo recuperación (copias de seguridad backup)	✓		✓		✓		
18	Existe un salvaguardas de tipo monitorización (registros de descargas de la web)	✓		✓		✓		

19	Existe un salvaguardas de tipo detección (antivirus, detectores de incendios, etc.)	✓		✓		✓		
20	Existe un salvaguardas de tipo concientización (cursos de concientización, cursos de formación, etc.)	✓		✓		✓		
21	Existe un salvaguardas de tipo administración (inventario de activos, plan de continuidad)	✓		✓		✓		
22	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia):
SI HAY

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: LUIS TORRES CABANILLAS **DNI:** 08904650

Especialidad del validador: ING. GEOTECNICO

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de Junio del 2019

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTIÓN DE RIESGOS

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. ACTIVOS DE INFORMACIÓN	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Existe un inventario de activos de información de la información esencial que maneja	✓		✓		✓		
2	Se tiene identificado los niveles o dependencias de los activos esenciales de información según la información que se maneja	✓		✓		✓		
3	El equipamiento informático depende del software, hardware, comunicaciones , soporte de información identificados en el inventario de activos de información de TI	✓		✓		✓		
	II. AMENAZAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
4	Se ha identificado adecuadamente las amenazas de origen natural (terremotos, inundaciones, etc.)	✓		✓		✓		
5	Se ha identificado adecuadamente las amenazas de origen industrial (contaminación, fallos eléctricos, etc.)	✓		✓		✓		
6	Se ha identificado adecuadamente las amenazas de defectos de las aplicaciones	✓		✓		✓		
7	Se ha identificado adecuadamente las amenazas causadas por personas de forma accidental	✓		✓		✓		
8	Se ha identificado adecuadamente las amenazas causadas por personas de forma deliberada	✓		✓		✓		
	III.IMPACTO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	

9	Se ha calculado el impacto acumulado, teniendo en cuenta su valor acumulado y las amenazas a las que está expuesto.	✓		✓		✓		
10	Se ha calculado el impacto repercutido teniendo en cuenta su valor propio y las amenazas a que están expuestos los activos de los que depende	✓		✓		✓		
	IV. RIESGO POTENCIAL	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Se ha calculado el riesgo acumulado por cada activo de información	✓		✓		✓		
12	Se ha calculado el riesgo repercutido por cada activo de información	✓		✓		✓		
	V. SALVAGUARDAS	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
13	Existen procedimientos o mecanismos tecnológicos que reducen el riesgo	✓		✓		✓		
14	Existe un salvaguardas de tipo preventiva (autorización previa de los usuarios, gestión de privilegios, planificación de capacidades, etc.)	✓		✓		✓		
15	Existe un salvaguardas de tipo eliminación de incidente impidiendo que éste tenga lugar (eliminación de cuentas estándar, de cuentas sin contraseña, de servicios innecesarios, etc.)	✓		✓		✓		
16	Existe un salvaguardas de tipo correctiva (gestión de incidentes)	✓		✓		✓		
17	Existe un salvaguardas de tipo recuperación (copias de seguridad backup)	✓		✓		✓		
18	Existe un salvaguardas de tipo monitorización (registros de descargas de la web)	✓		✓		✓		

19	Existe un salvaguardas de tipo detección (antivirus, detectores de incendios, etc.)	✓		✓		✓		
20	Existe un salvaguardas de tipo concientización (cursos de concientización, cursos de formación, etc.)	✓		✓		✓		
21	Existe un salvaguardas de tipo administración (inventario de activos, plan de continuidad)	✓		✓		✓		
22	Existen las sanciones por incumplimiento de la ley u obligaciones contractuales	✓		✓		✓		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: DR. PADILLA CABALLERO, JESUS **DNI:** 25861074

Especialidad del validador: METODÓLOGO

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de JUNIO del 2019

Firma del Experto Informante
Dr. Jesús Emilio Agustín Padilla Caballero
CPPe. 0125861074

Anexo 6: Certificado de validez de los instrumentos de la variable Seguridad de la Información

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFOMACIÓN

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. CONFIDENCIALIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información							
2	Se cuenta con un adecuado inventario de los accesos a los sistemas							
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)							
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios							
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información							
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos							
	II. INTEGRIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
7	Cuentan con políticas de intercambio de información ya sea física o electrónica							
8	No generan copias de seguridad en la nube de la información propia de la empresa							
9	Realizan controles en la red							

10	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales							
	III. DISPONIBILIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
11	Existe un plan de contingencia contra desastres que pongan en riesgo la información							
12	Cuentan con políticas de restauración segura de backups de información							
13	Se cuenta con Directivas o procedimientos para acceder a la información							
14	Existen restricciones para disponer de la información							

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: ……DNI:…….

Especialidad del validador:……..

1Pertinencia: El ítem corresponde al concepto teórico formulado.

2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo

3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

…….de……..del 20…..

_____

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFOMACIÓN

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. CONFIDENCIALIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	✓		✓		✓		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	✓		✓		✓		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	✓		✓		✓		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	✓		✓		✓		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	✓		✓		✓		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	✓		✓		✓		
	II. INTEGRIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	✓		✓		✓		
8	Generan copias de seguridad en la nube de la información propia de la empresa	✓		✓		✓		
9	Realizan controles en la red	✓		✓		✓		
10	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	✓		✓		✓		

	III. DISPONIBILIDAD	Sí	No	Sí	No	Sí	No	
11	Existe un plan de contingencia contra desastres que pongan en riesgo la información	✓		✓		✓		
12	Cuentan con políticas de restauración segura de backups de información	✓		✓		✓		
13	Se cuenta con Directivas o procedimientos para acceder a la información	✓		✓		✓		
14	Existen restricciones para disponer de la información	✓		✓		✓		

Observaciones (precisar si hay suficiencia):
SI HAY

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: LUIS TORRES CABANILLAS **DNI:** 08404660

Especialidad del validador: Ing. ESTADISTICO CIP 45863

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de JUNIO del 2019

Firma del Experto Informante

UCV
UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFOMACIÓN

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. CONFIDENCIALIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	✓		✓		✓		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	✓		✓		✓		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	✓		✓		✓		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	✓		✓		✓		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	✓		✓		✓		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	✓		✓		✓		
	II. INTEGRIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	✓		✓		✓		
8	Generan copias de seguridad en la nube de la información propia de la empresa	✓		✓		✓		
9	Realizan controles en la red	✓		✓		✓		
10	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	✓		✓		✓		

	III. DISPONIBILIDAD	Sí	No	Sí	No	Sí	No	
11	Existe un plan de contingencia contra desastres que pongan en riesgo la información	✓		✓		✓		
12	Cuentan con políticas de restauración segura de backups de información	✓		✓		✓		
13	Se cuenta con Directivas o procedimientos para acceder a la información	✓		✓		✓		
14	Existen restricciones para disponer de la información	✓		✓		✓		

Observaciones (precisar si hay suficiencia): EXISTE SUFICIENCIA

Opinión de aplicabilidad: Aplicable [✓] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: ...Dr. PADILLA CASDULERO, JESUS.....**DNI:**.....25861074...

Especialidad del validador:.....METODÓLOGO.....

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

.....15.....de.....Junio.....del 20.19.

Firma del Experto Informante
Dr. Jesus Emilio Agustin Padilla Caballero
CPPe. 0125881074

UCV
UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA SEGURIDAD DE LA INFOMACIÓN

N°	Dimensiones / Ítems	Pertinencia		Relevancia		Claridad		Sugerencias
	I. CONFIDENCIALIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
1	Se cuenta con políticas efectivas donde se administre y controle los accesos a la información	✓		✓		✓		
2	Se cuenta con un adecuado inventario de los accesos a los sistemas	✓		✓		✓		
3	Se cuenta con tecnologías de autentificación de usuario (verificación de huellas o firmas)	✓		✓		✓		
4	Se utilizan métodos apropiados de autentificación para el control de acceso de usuarios	✓		✓		✓		
5	Se cuenta con documentación clara de los niveles de autorización de acceso a la información	✓		✓		✓		
6	Se manejan procedimientos para la autorización formal de solicitudes de accesos	✓		✓		✓		
	II. INTEGRIDAD	**Sí**	**No**	**Sí**	**No**	**Sí**	**No**	
7	Cuentan con políticas de intercambio de información ya sea física o electrónica	✓		✓		✓		
8	Generan copias de seguridad en la nube de la información propia de la empresa	✓		✓		✓		
9	Realizan controles en la red	✓		✓		✓		
10	Se cuenta con herramientas adecuadas para la protección contra amenazas externas y ambientales	✓		✓		✓		

	III. DISPONIBILIDAD	Sí	No	Sí	No	Sí	No	
11	Existe un plan de contingencia contra desastres que pongan en riesgo la información	✓		✓		✓		
12	Cuentan con políticas de restauración segura de backups de información	✓		✓		✓		
13	Se cuenta con Directivas o procedimientos para acceder a la información	✓		✓		✓		
14	Existen restricciones para disponer de la información	✓		✓		✓		

Observaciones (precisar si hay suficiencia):

Si hay

Opinión de aplicabilidad: Aplicable [X] **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: Cano Hernández Yolly **DNI:** 40043433

Especialidad del validador: Mg. en Investigación

1Pertinencia: El ítem corresponde al concepto teórico formulado.
2Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
3Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

15 de junio del 2019

Firma del Experto Informante

Anexo 7: Matriz de datos

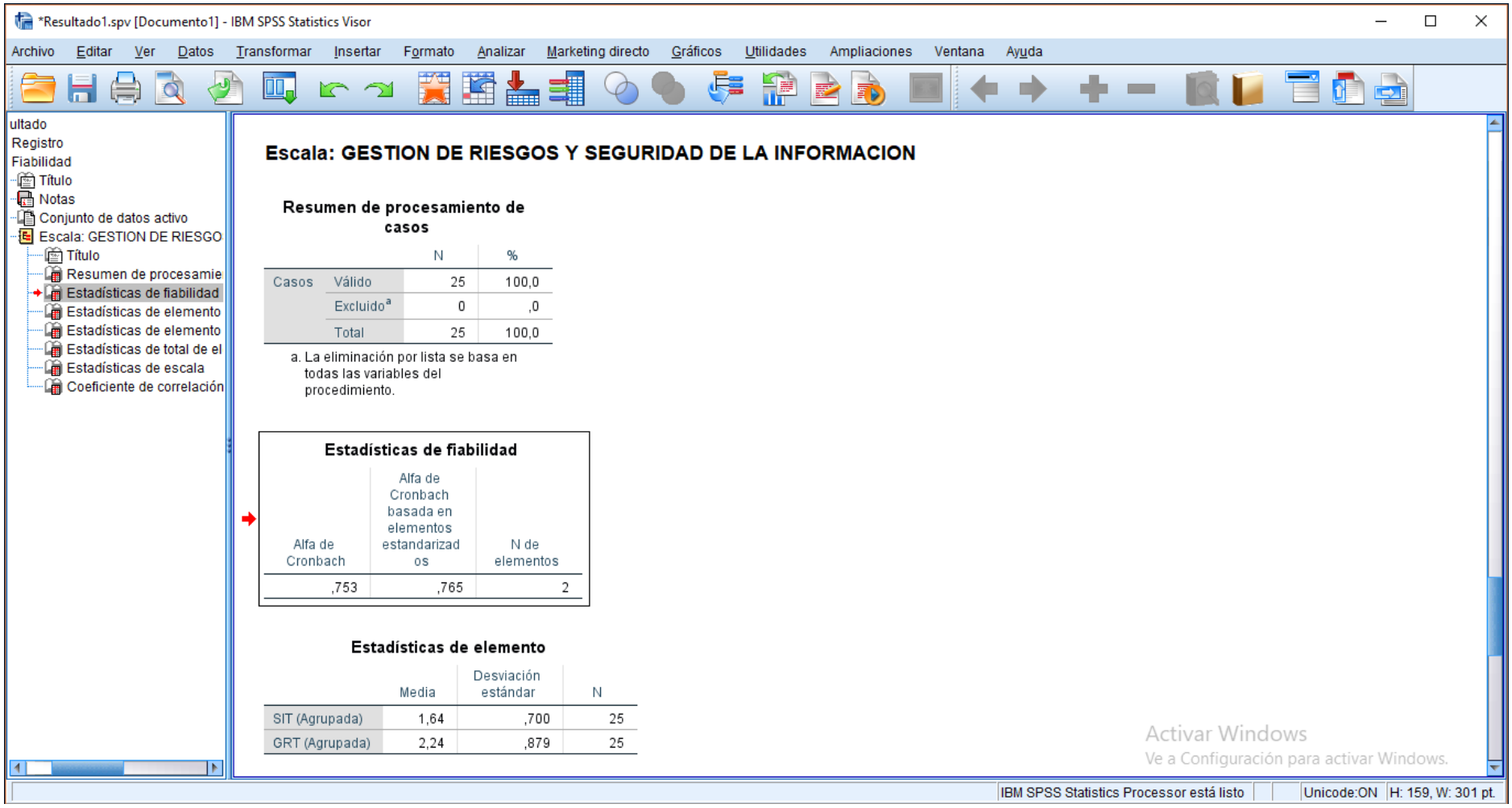
	Gestión de riesgos																											
N°	Activos de información			Amenazas					Impacto potencial		Riesgo potencial		Salvaguardas										V1	D1	D2	D3	D4	D5
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	T					
1	1	1	1	2	2	1	1	1	1	1	1	1	1	2	2	1	1	2	1	2	2	1	29	3	7	2	2	15
2	2	2	2	1	1	1	1	1	2	2	2	2	1	1	1	2	2	2	2	2	2	1	35	6	5	4	4	16
3	3	2	2	2	2	2	2	2	3	2	3	2	2	2	3	3	3	3	3	3	3	2	54	7	10	5	5	27
4	4	4	4	4	3	2	2	2	4	3	4	3	1	1	2	2	2	4	2	2	2	1	58	12	13	7	7	19
5	2	2	2	2	2	2	2	2	2	2	2	2	1	2	3	3	3	3	3	3	3	1	49	6	10	4	4	25
6	3	2	2	2	2	3	3	3	3	3	3	3	2	3	3	2	3	3	3	3	3	1	58	7	13	6	6	26
7	2	2	2	2	2	2	2	2	2	3	2	3	2	2	3	3	3	4	3	3	3	2	54	6	10	5	5	28
8	2	3	3	2	2	3	2	3	3	2	3	2	2	2	2	2	3	3	3	3	3	2	55	8	12	5	5	25
9	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	43	6	10	4	4	19
10	3	3	3	2	2	2	3	3	3	3	3	3	2	2	3	2	3	3	3	3	3	1	58	9	12	6	6	25
11	2	2	2	2	2	2	1	2	2	2	2	2	1	1	1	2	2	2	2	2	2	1	39	6	9	4	4	16
12	2	2	2	2	2	2	2	2	3	3	3	3	2	2	2	2	2	2	2	2	2	2	48	6	10	6	6	20
13	3	2	3	2	2	3	3	3	3	3	3	3	2	2	3	3	3	3	3	3	3	2	60	8	13	6	6	27

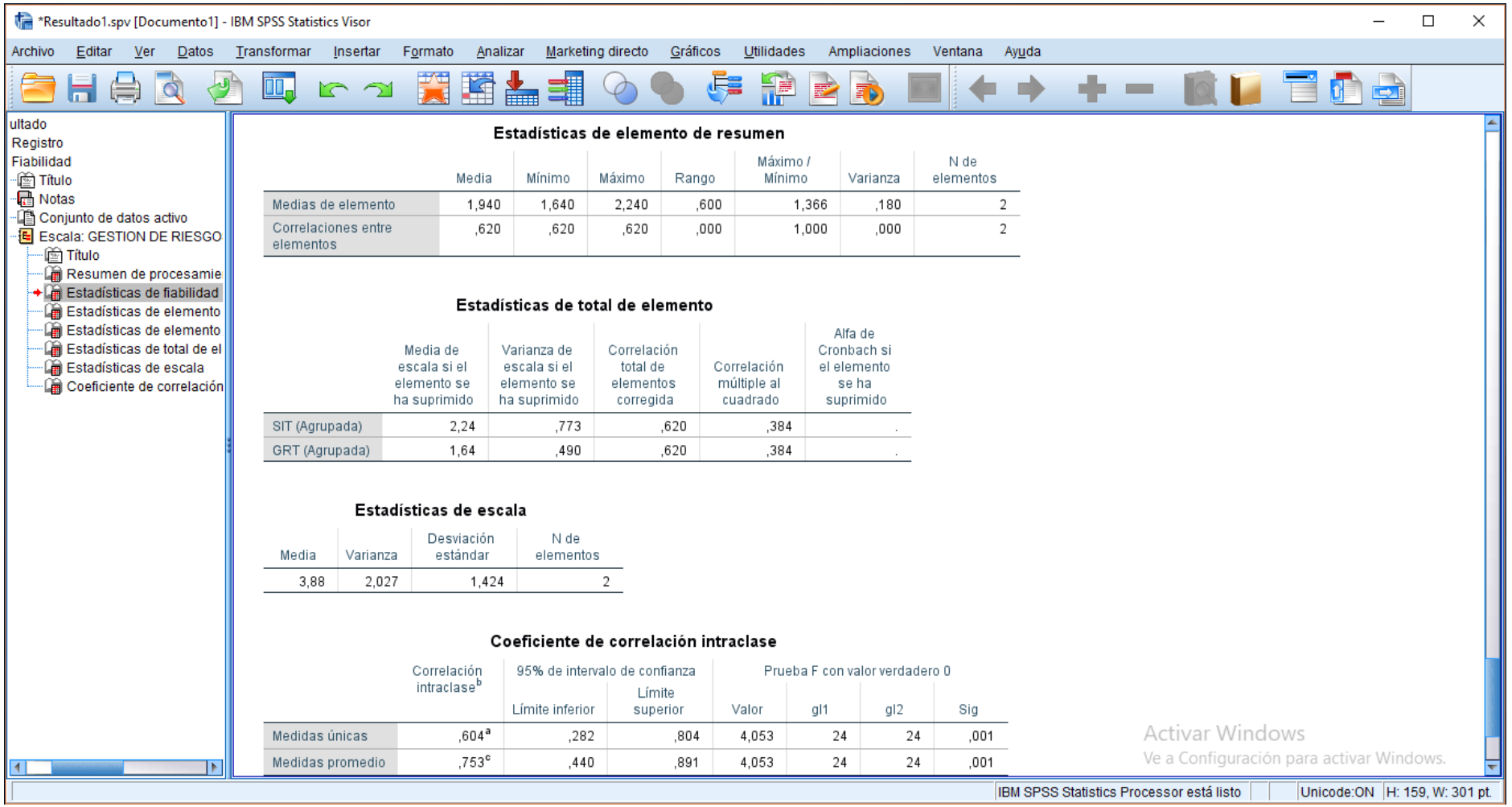
14	2	2	2	2	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1	42	6	10	4	4	18
15	3	2	3	3	2	3	2	3	3	3	3	3	2	2	3	2	3	3	3	3	3	2	59	8	13	6	6	26
16	3	2	3	2	3	3	2	3	2	2	2	2	2	2	3	3	3	2	3	3	3	2	55	8	13	4	4	26
17	1	3	2	1	1	1	1	1	2	2	2	2	1	2	2	1	1	2	1	2	2	1	34	6	5	4	4	15
18	2	2	2	2	2	2	2	2	4	3	4	3	2	2	2	2	2	2	2	2	2	2	50	6	10	7	7	20
19	3	3	3	3	2	2	3	3	2	2	2	2	2	2	3	2	3	3	3	3	3	2	56	9	13	4	4	26
20	2	3	3	2	3	2	2	2	3	3	3	3	2	2	3	2	3	3	3	3	3	2	57	8	11	6	6	26
21	1	3	2	1	2	2	1	1	1	1	1	1	1	2	2	1	1	3	1	2	2	1	33	6	7	2	2	16
22	1	3	2	1	1	2	1	2	2	2	2	2	1	2	2	1	1	3	1	2	2	1	37	6	7	4	4	16
23	2	3	3	2	3	3	2	3	3	3	3	3	3	2	2	2	2	2	2	2	2	2	54	8	13	6	6	21
24	2	2	2	1	2	2	2	2	1	1	1	1	1	1	2	2	2	2	2	2	2	1	36	6	9	2	2	17
25	2	2	2	1	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	1	41	6	9	4	4	18

	Seguridad de la Información																	
N°	Confiabilidad						Integridad				Disponibilidad				V2	D1	D2	D3
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	T			
1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	16	8	4	4
2	2	1	3	2	2	3	1	1	2	1	1	1	2	1	23	13	5	5
3	2	2	2	3	3	2	1	1	2	2	1	1	2	1	25	14	6	5
4	2	4	2	2	2	4	3	2	4	3	3	3	4	3	41	16	12	13
5	2	1	3	2	2	2	2	1	4	2	2	1	4	1	29	12	9	8
6	2	2	2	2	2	2	2	1	2	3	2	1	2	1	26	12	8	6
7	2	4	2	2	3	4	3	3	4	3	3	3	4	3	43	17	13	13
8	2	2	3	3	2	2	2	2	2	3	1	2	2	3	31	14	9	8
9	2	1	2	2	2	2	2	1	2	2	1	1	2	1	23	11	7	5
10	2	2	2	3	2	2	2	2	2	2	2	2	2	2	29	13	8	8
11	1	2	2	2	2	2	2	2	2	2	1	2	2	1	25	11	8	6
12	1	1	2	2	2	2	2	1	1	2	1	1	1	1	20	10	6	4
13	2	2	2	3	3	2	3	2	2	3	3	2	2	3	34	14	10	10
14	1	1	2	2	2	2	2	1	2	2	2	1	2	2	24	10	7	7
15	2	2	3	3	2	2	2	2	2	2	2	2	2	2	30	14	8	8
16	2	3	2	3	2	2	3	2	2	3	1	2	2	3	32	14	10	8
17	1	1	2	2	2	2	3	1	3	3	1	1	3	1	26	10	10	6
18	1	1	2	2	2	2	2	1	1	2	1	1	1	1	20	10	6	4
19	3	2	3	3	2	3	3	2	3	3	3	2	3	3	38	16	11	11
20	2	3	2	2	2	2	3	2	2	3	3	2	2	3	33	13	10	10
21	2	1	2	2	2	2	3	1	2	3	1	1	2	1	25	11	9	5
22	2	1	2	2	2	2	2	1	2	2	1	1	2	1	23	11	7	5
23	2	2	3	3	2	3	2	1	2	2	2	1	2	2	29	15	7	7
24	1	1	2	2	2	2	1	1	1	2	1	1	1	1	19	10	5	4
25	1	1	2	2	2	1	1	2	1	2	1	2	1	1	20	9	6	5

Anexo 8: Tablas y gráficos alternos del capítulo resultados

Análisis de fiabilidad de las variables Gestión de Riesgos y Seguridad de la Información





Estadísticas de elemento de resumen

	Media	Mínimo	Máximo	Rango	Máximo / Mínimo	Varianza	N de elementos
Medias de elemento	1,940	1,640	2,240	,600	1,366	,180	2
Correlaciones entre elementos	,620	,620	,620	,000	1,000	,000	2

Estadísticas de total de elemento

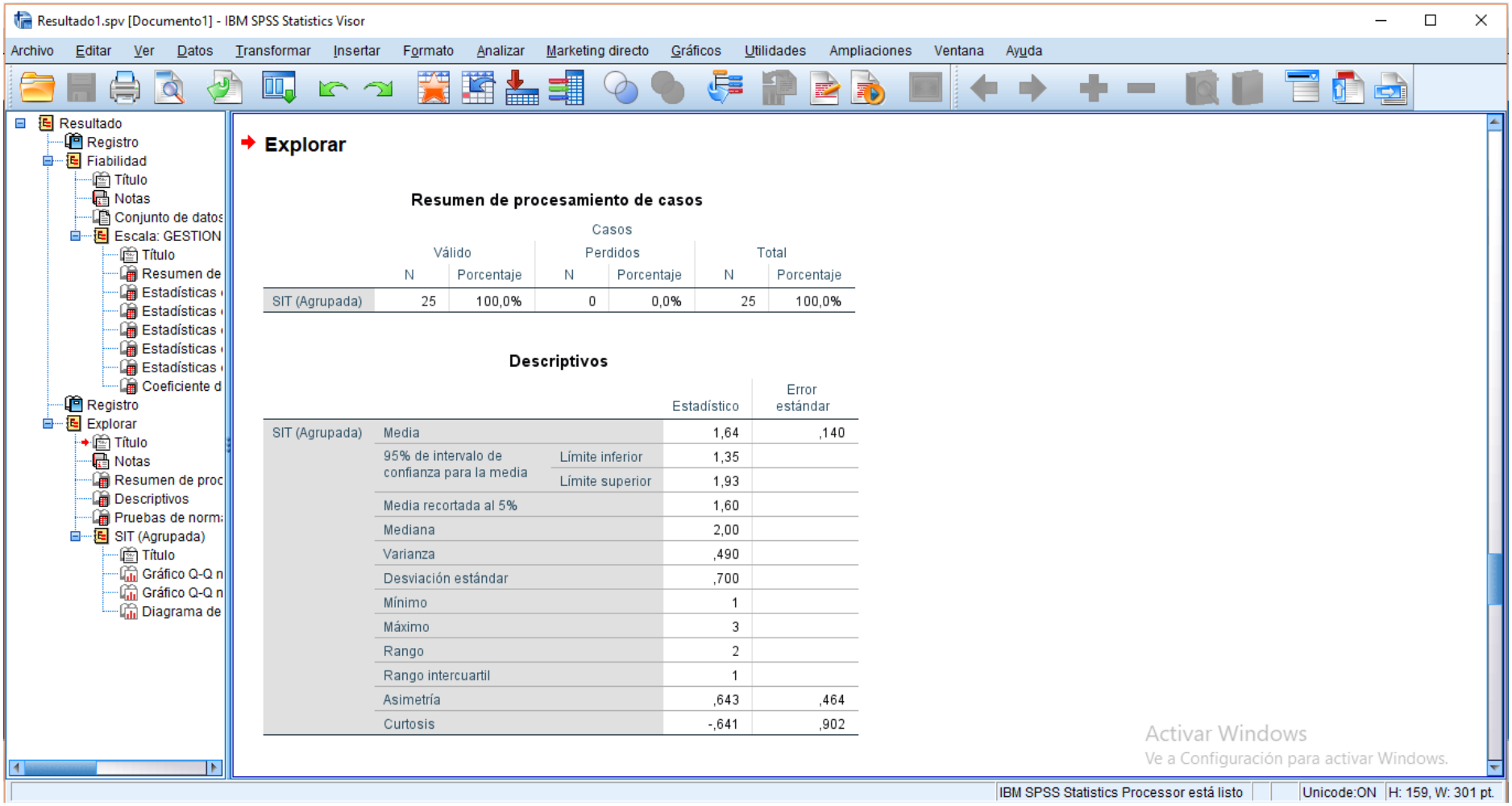
	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Correlación múltiple al cuadrado	Alfa de Cronbach si el elemento se ha suprimido
SIT (Agrupada)	2,24	,773	,620	,384	.
GRT (Agrupada)	1,64	,490	,620	,384	.

Estadísticas de escala

Media	Varianza	Desviación estándar	N de elementos
3,88	2,027	1,424	2

Coeficiente de correlación intraclase

	Correlación intraclase[b]	95% de intervalo de confianza		Prueba F con valor verdadero 0			
		Límite inferior	Límite superior	Valor	gl1	gl2	Sig
Medidas únicas	,604[a]	,282	,804	4,053	24	24	,001
Medidas promedio	,753[c]	,440	,891	4,053	24	24	,001


Resultado1.spv [Documento1] - IBM SPSS Statistics Visor
Archivo Editar Ver Datos Transformar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ampliaciones Ventana Ayuda
Resultado
Registro
Fiabilidad
Título
Notas
Conjunto de datos
Escala: GESTION
Título
Resumen de
Estadísticas
Estadísticas
Estadísticas
Estadísticas
Estadísticas
Coeficiente d
Registro
Explorar
Título
Notas
Resumen de proc
Descriptivos
Pruebas de norm
SIT (Agrupada)
Título
Gráfico Q-Q n
Gráfico Q-Q n
Diagrama de
Explorar
Resumen de procesamiento de casos
Casos
Válido
Perdidos
Total
N
Porcentaje
N
Porcentaje
N
Porcentaje
SIT (Agrupada) 25 100,0% 0 0,0% 25 100,0%
Descriptivos
Estadístico
Error estándar
SIT (Agrupada) Media 1,64 ,140
95% de intervalo de confianza para la media Límite inferior 1,35
Límite superior 1,93
Media recortada al 5% 1,60
Mediana 2,00
Varianza ,490
Desviación estándar ,700
Mínimo 1
Máximo 3
Rango 2
Rango intercuartil 1
Asimetría ,643 ,464
Curtosis -,641 ,902
Activar Windows
Ve a Configuración para activar Windows.
IBM SPSS Statistics Processor está listo
Unicode:ON
H: 159, W: 301 pt.

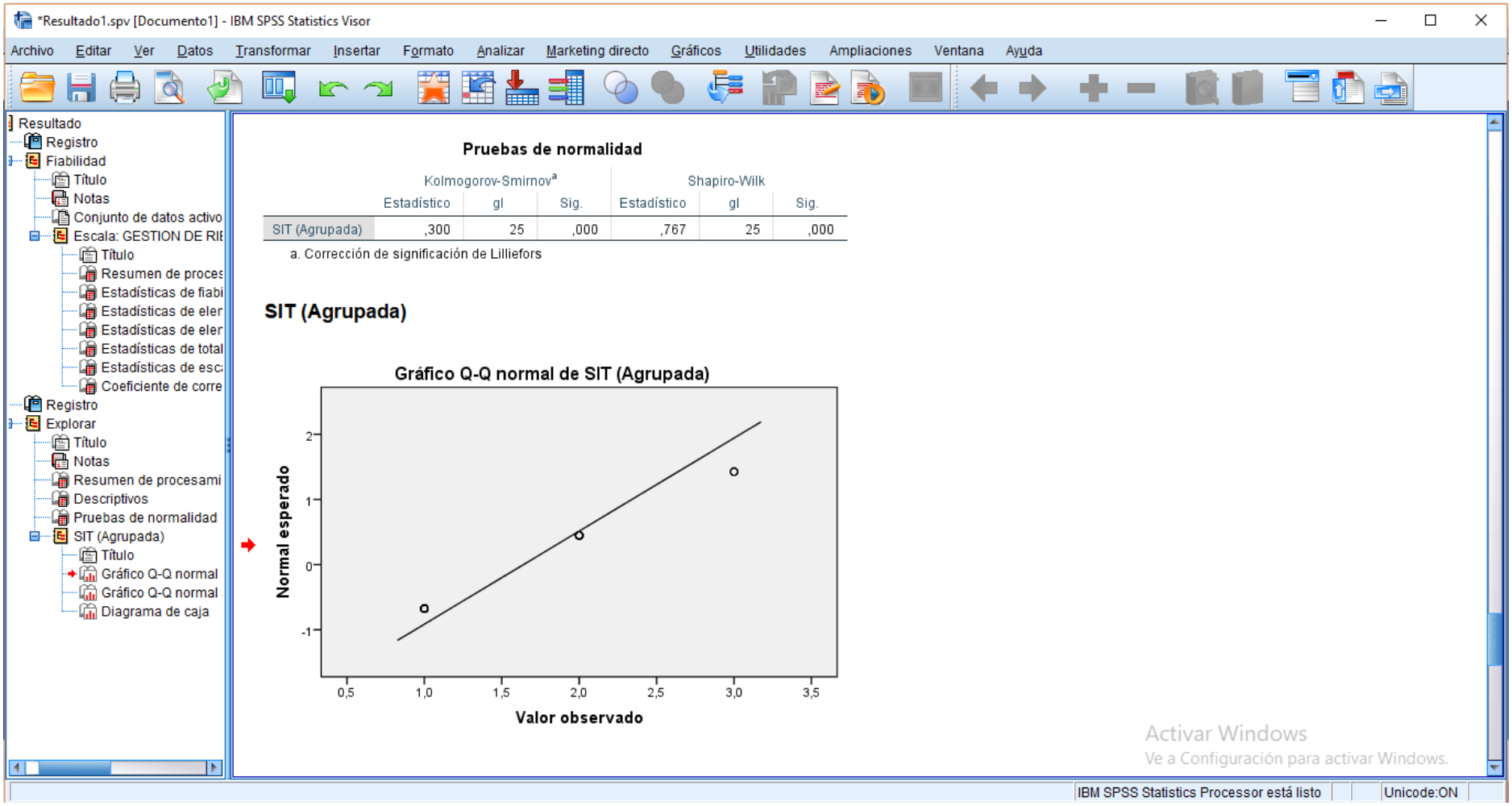
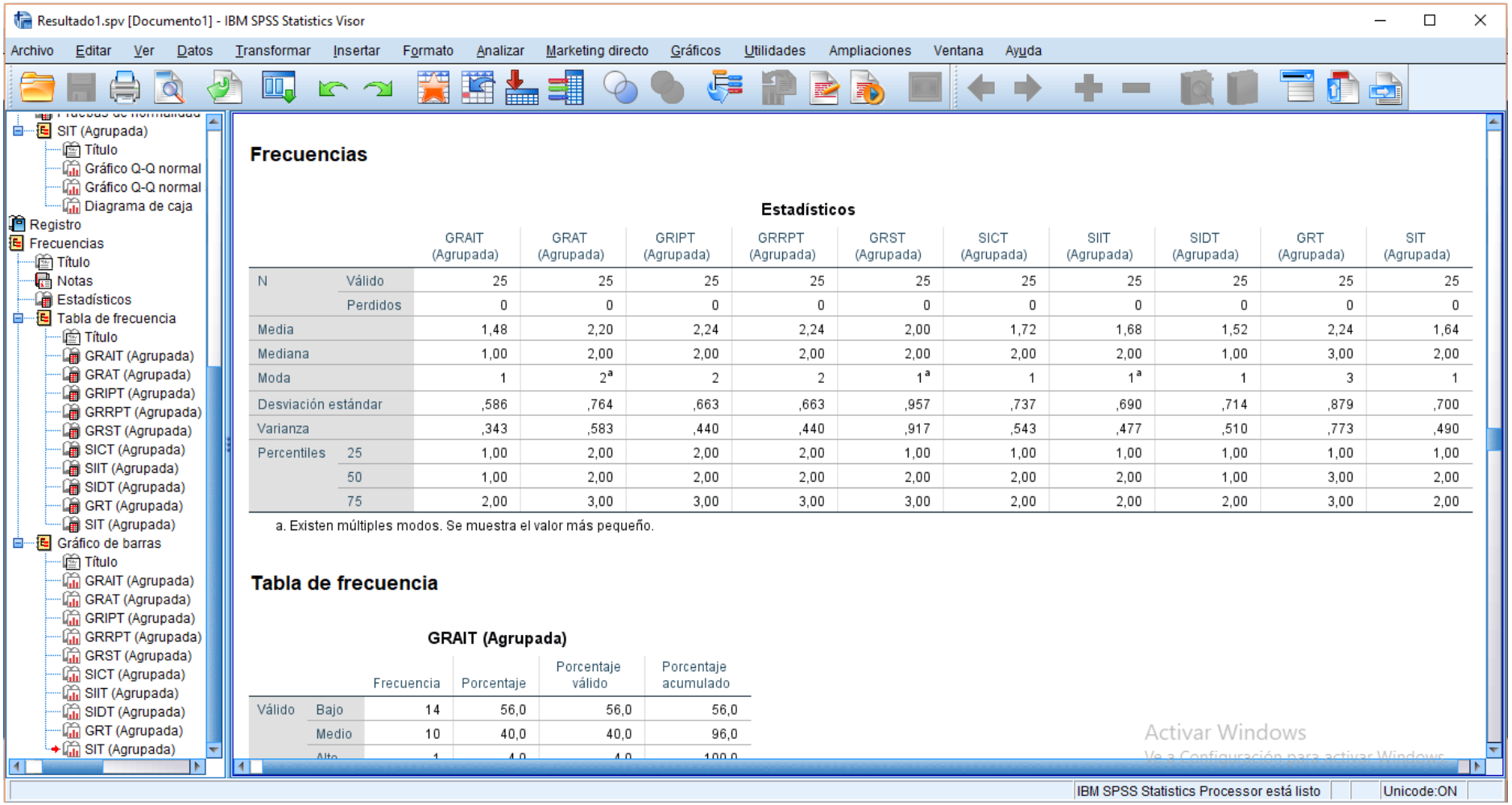
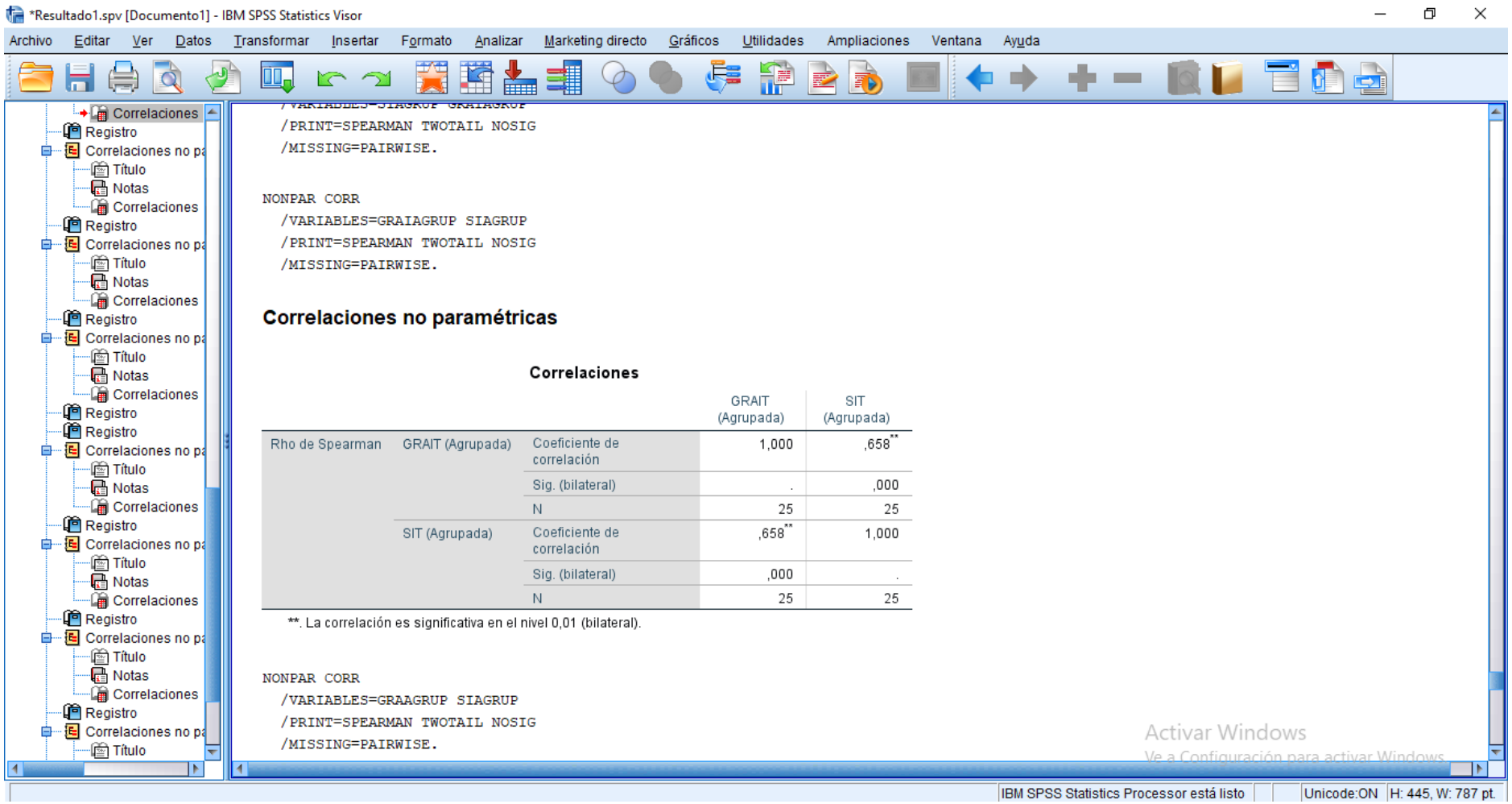

*Resultado1.spv [Documento1] - IBM SPSS Statistics Visor
Archivo Editar Ver Datos Transformar Insertar Formato Analizar Marketing directo Gráficos Utilidades Ampliaciones Ventana Ayuda
Resultado
Registro
Fiabilidad
Título
Notas
Conjunto de datos activo
Escala: GESTION DE RIE
Título
Resumen de proces
Estadísticas de fiabi
Estadísticas de eler
Estadísticas de eler
Estadísticas de total
Estadísticas de esc
Coeficiente de corre
Registro
Explorar
Título
Notas
Resumen de procesami
Descriptivos
Pruebas de normalidad
SIT (Agrupada)
Título
Gráfico Q-Q normal
Gráfico Q-Q normal
Diagrama de caja
Pruebas de normalidad
Kolmogorov-Smirnov[a] Shapiro-Wilk
Estadístico gl Sig. Estadístico gl Sig.
SIT (Agrupada) ,300 25 ,000 ,767 25 ,000
a. Corrección de significación de Lilliefors
SIT (Agrupada)
Gráfico Q-Q normal de SIT (Agrupada)
Normal esperado
Valor observado
2
1
0
-1
0,5
1,0
1,5
2,0
2,5
3,0
3,5
Activar Windows
Ve a Configuración para activar Windows.
IBM SPSS Statistics Processor está listo
Unicode:ON

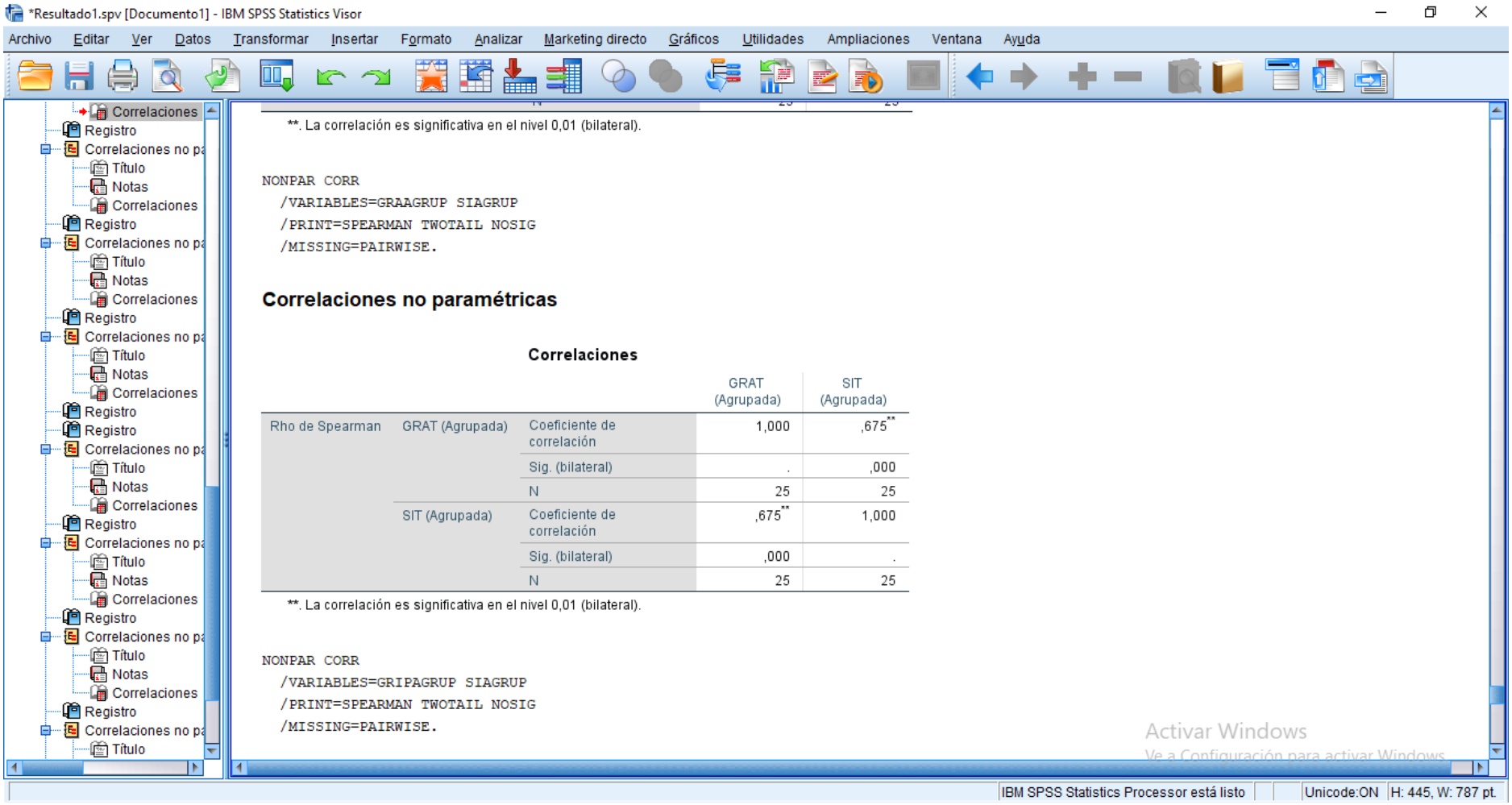
Tabla de Frecuencias



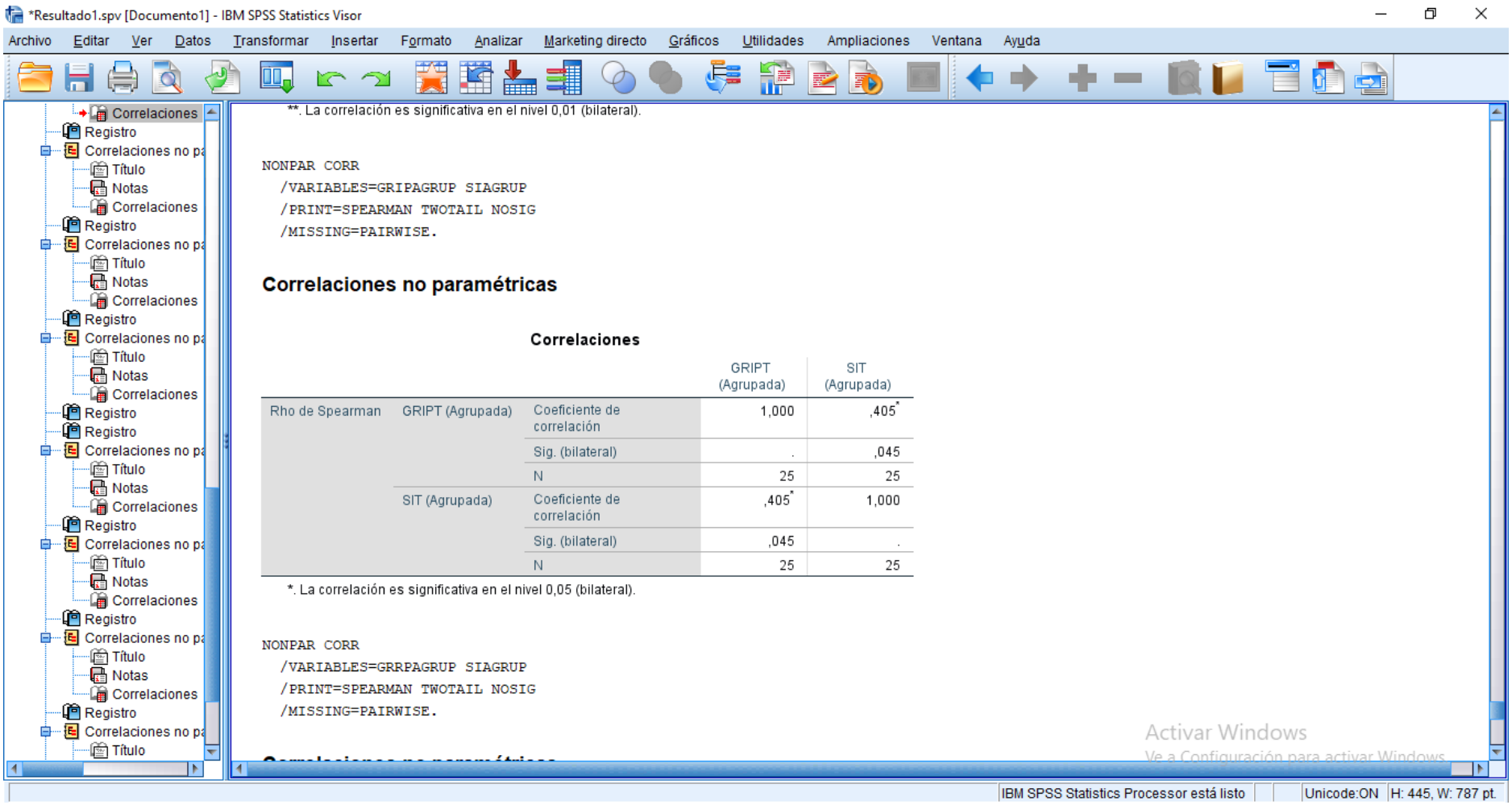
Correlación de Dimensión Activos de Información y Seguridad de la Información



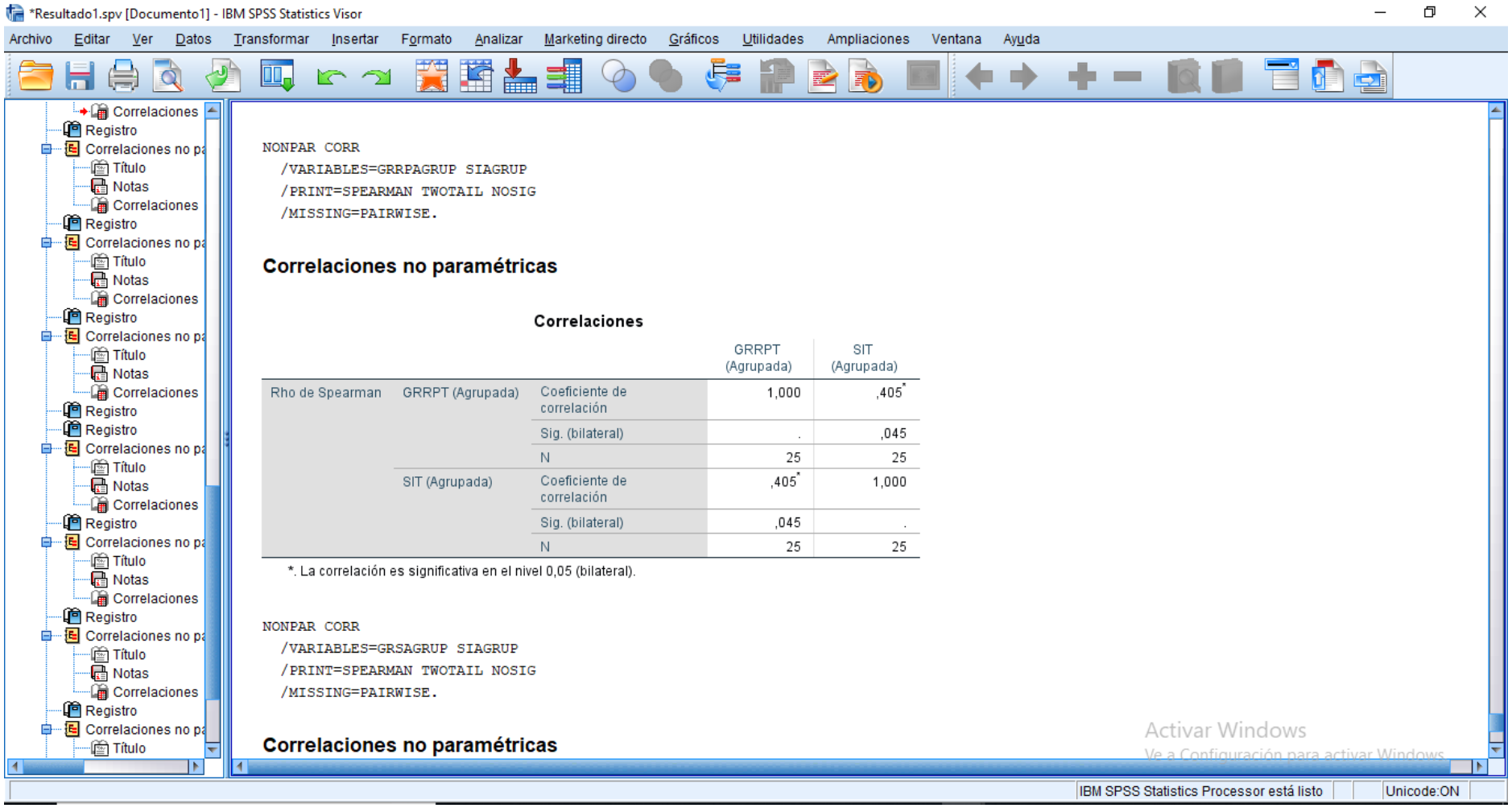
Correlación de Dimensión Amenazas y Seguridad de la Información



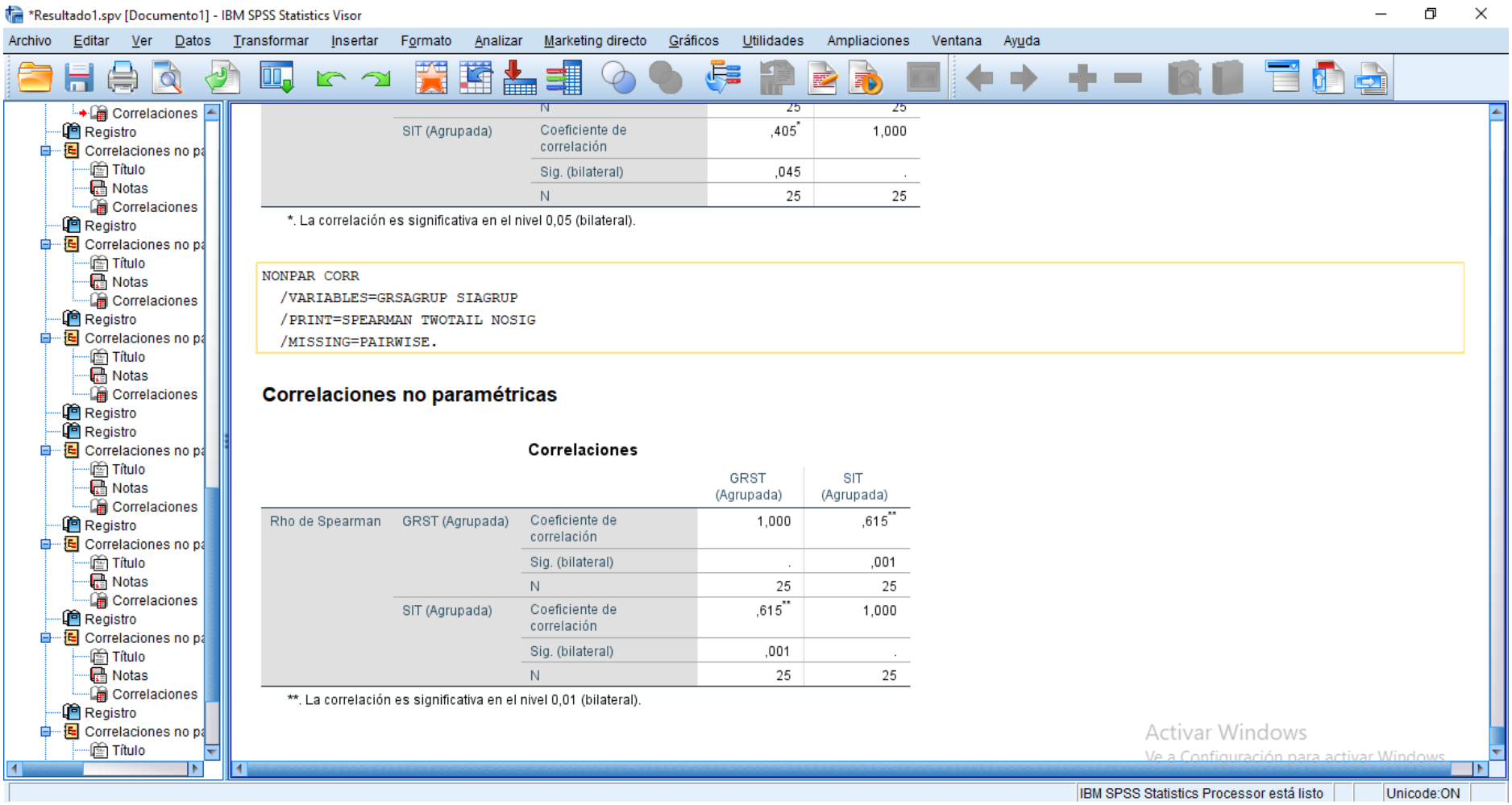
Correlación de Dimensión Impacto potencial y Seguridad de la Información



Correlación de Dimensión Riesgo potencial y Seguridad de la Información



Correlación de Dimensión Salvaguardas y Seguridad de la Información



Anexo 9: Resultado de la propuesta

	Gestión de riesgos																											
N°	Activos de información			Amenazas					Impacto potencial		Riesgo potencial		Salvaguardas										V1	D1	D2	D3	D4	D5
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	T					
1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
4	5	5	5	5	4	4	4	4	5	5	5	5	4	4	4	4	4	5	4	4	4	5	98	15	21	10	10	42
5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
6	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
7	5	5	5	5	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	93	15	21	8	8	41
8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
9	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
10	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
11	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
12	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40

13	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
14	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	90	13	20	8	8	41
15	4	4	4	4	4	4	4	4	5	4	4	5	4	4	4	4	4	4	4	4	4	4	90	12	20	9	9	40
16	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
17	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
18	4	4	4	4	4	4	4	4	5	5	5	5	4	4	4	4	4	4	4	4	4	4	92	12	20	10	10	40
19	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
20	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
21	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	89	13	20	8	8	40
22	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
23	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	89	12	20	9	8	40
24	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	88	12	20	8	8	40
25	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	90	13	20	8	8	41

	Seguridad de la Información																	
N°	Confiabilidad						Integridad				Disponibilidad				V2	D1	D2	D3
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	T			
1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
4	4	5	4	4	4	5	4	4	4	4	4	4	5	5	60	26	16	18
5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
6	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
7	5	4	5	4	4	4	4	4	4	4	4	4	4	4	58	26	16	16
8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
9	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
10	4	4	4	4	4	4	4	4	4	4	4	4	5	4	57	24	16	17
11	4	4	5	4	4	4	4	4	4	4	4	4	4	4	57	25	16	16
12	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
13	4	4	4	4	4	5	4	4	4	4	4	4	5	4	58	25	16	17
14	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
15	4	4	4	4	4	4	4	4	4	4	4	4	5	4	57	24	16	17
16	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
17	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
18	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
19	5	4	4	4	4	4	4	4	4	4	4	4	4	4	57	25	16	16
20	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
21	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
22	4	4	5	4	4	4	4	4	4	4	4	4	4	4	57	25	16	16
23	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
24	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16
25	4	4	4	4	4	4	4	4	4	4	4	4	4	4	56	24	16	16